Post-Privacy

Gesellschaftliche Chancen und Risiken einer aufkeimenden Transparenzkultur

Masterthesis zur Erlangung des akademischen Grades
„Master of Arts in Arts and Design“

Verfasser
Georg Pircher Verdorfer

Vorgelegt am FH-Studiengang MultiMediaArt, Fachhochschule Salzburg

BetreuerInnen
Dr. Felix Kramer
Mag.a Gabriele Neudecker

Salzburg, 07. Mai 2013

Eidesstattliche Erklärung

Hiermit versichere ich, Georg Pircher Verdorfer, geboren am 08. Mai 1984 in Meran (Italien), dass ich die Grundsätze wissenschaftlichen Arbeitens nach bestem Wissen und Gewissen eingehalten habe und die vorliegende Masterthesis von mir selbstständig verfasst wurde. Zur Erstellung wurden von mir keine anderen als die angegebenen Quellen und Hilfsmittel verwendet.

Ich versichere, dass ich die Masterthesis weder im In- noch Ausland bisher in irgendeiner Form als Prüfungsarbeit vorgelegt habe und dass diese Arbeit mit der den BegutachterInnen vorgelegten Arbeit übereinstimmt.

Salzburg, am 07. Mai 2013

0910627015

Georg Pircher Verdorfer Matrikelnummer

Kurzfassung der Arbeit

Verfasser: Georg Pircher Verdorfer
Institution: Fachhochschule Salzburg
Studiengang: MultiMediaArt
Titel: Post-Privacy
Betreuer 1: Dr. Felix Kramer
Betreuerin 2: Mag.a Gabriele Neudecker
Schlagwörter: Post-Privacy, Transparenz, Datenschutz

Ganz nebenbei sind wir eingetreten in die Welt der Bits und Bytes. Dank smarter Mobiltelefone können wir buchstäblich auf Schritt und Tritt verfolgt werden. Mit jeder Lebensäußerung auf Social Networks, bereichern wir irgendwo einen Datenpool, der analysiert, gefiltert und interpretiert werden kann. Die Verdatung der Gesellschaft macht vor kaum einem Lebensbereich mehr halt.

Ganz nebenbei zerfranst im Zuge dieser Verdatung auch ein Konstrukt, welches bis dato als unantastbares Grundrecht in allen modernen Demokratien, als fest verankert galt: Das Recht auf Privatsphäre. Doch angesichts der Offenheit und Unbekümmertheit mit welcher private Fragmente zunehmend ihren Weg in die Öffentlichkeit finden, scheint dieses Recht kaum noch eingefordert zu werden. ‚Transparenz statt Privatsphäre' lautet das Diktum der Post-Privacy, dem Zeitalter nach der Privatsphäre.

Die möglichen Auswirkungen dieses transparenten Umfelds auf die Gesellschaft, stellen das Forschungsinteresse der vorliegenden Arbeit dar. In der Gegenüberstellung der Argumentationen ihrer BefürworterInnen und SkeptikerInnen werden die vielen Risiken aber eben auch Chancen der Post-Privacy aufgezeigt.

Abstract

Not even noticing, we have entered the world of bits and bytes. Thanks to smart phones, every step we take is tracked. With each single life-expression in social networks more and more personal data are stored, which will be analysed, filtered and interpreted in some way. The cross-linking of society does barley spare an area of life.

At the same time, as a by-product of this cross-linking, a long sacrosanct fundamental right and a highly esteemed value of our democratic societies gets dismantled piecemeal: The right to privacy. But given the openness and unconcern, private fragments are progressively becoming available to the public, hardly anybody seems to claim this right anymore. ‚Transparency instead of Privacy' reads the dictum of Post-Privacy, the era after privacy protection.

This Master's Thesis investigates the possible consequences of a transparent environment to our society. In the examination of arguments from proponents and sceptics, the possible risks and opportunities of Post-Privacy are revealed.

Abkürzungsverzeichnis

Anm. d. Verf.	Anmerkung des/der Verfassers/Verfasserin
d.h.	das heißt
etc.	et cetera
f	und folgende Seiten
ff	und folgende Seiten
ggf.	gegebenenfalls
IMHO	In my humble opinion
resp.	respektive
sog.	sogenannt
usw.	und so weiter
vs.	versus
z.B.	zum Beispiel
z.T.	zum Teil

Inhaltsverzeichnis

Einleitung

> Privacy is dead and social media hold the smoking gun.
> (Cashmore 2009: online)

Die Privatsphäre wie wir sie heute kennen, fristet ein gefährdetes Dasein. Die zunehmende Verdatung und Vernetzung, die Überwachungspraxis von Staat und Konzernen, lassen ihr Gebilde langsam zerbröckeln. Wir können uns dagegen wehren, uns abschotten und in Datenaskese üben. Doch wenn wir nicht in einer Höhle leben wollen und uns auch nur hin und wieder ein wenig im Netz bewegen, müssen wir uns klar machen, dass wir damit einen Teil unserer Privatheit abtreten. Doch was kommt nach dem Ende der Privatsphäre, quasi posthum? Ich nenne dieses Zeitalter in der vorliegenden Arbeit 'Post-Privacy': das Leben nach der Privatsphäre.

Die Debatte darüber, die Post-Privacy-Debatte also, könnte man vergleichend wohl recht nahe an der Kapitalismus-Debatte führen. Auch Globalisierung, die Atomenergie etc. würden sich als Diskussions-Vergleich anbieten. Sie alle haben gemein, dass sie unter Gelehrten wie Gemeinen recht negativ konnotiert sind. Wer würde sich schon freiwillig einen 'Capitalizm rulz'- oder 'Post-Privacy-4ever'-Button an seine/ihre LKW-Planen-Tasche heften? Oder auch nur ein lobendes Wort über die Atomenergie[1] verlieren. Dennoch hat sich über die Jahrzehnte so etwas wie eine gesellschaftliche Akzeptanz, ganz zu schweigen von der weltweiten Abhängigkeit, eingebürgert. Gewisse Dinge, von denen wir profitieren, so klandestin deren Hintergründe auch erscheinen mögen, hinterfragen wir BürgerInnen des Okzidents am besten gar nicht. Im Konnex der Post-Privacy heißt das: „Obwohl Medien kritisch über

[1] angesichts der jüngsten Reaktorkatastrophen in Japan, käme ein löbliches Wort für die Atomkraftwerke fast einer Wiederbetätigung gleich.

Firmen wie Facebook, Google berichten, nutzen viele Menschen ihre Dienste, […] obwohl ihre Daten ausgewertet werden, um beispielsweise optimierte Werbung zu zeigen. Da übersteigt für viele Anwender der Nutzen die Kosten." (Geuter 2013: online) Ist die Post-Privacy ein Kind der Bequemlichkeit? Oder hinkt der Vergleich insgesamt? Kann man das Post-Privacy-Phänomen doch nicht zusammen mit Kapitalismus, Atomenergie und Konsorten unter den Hut des Bösen stecken?

Wie der Untertitel dieser Arbeit verrät, geht es darum, die gesellschaftlichen Risiken und Chancen einer Post-Privacy-Kultur darzulegen. Es liegt mir fern, einen argumentativen Feldzug gegen die Post-Privacy-VertreterInnen und ihre Positionen loszutreten. Ebensowenig möchte ich mich gegen die DatenschützerInnen mit ihrer Post-Privacy-kritischen Haltung stemmen. Ich versuche einen möglichst neutralen Überblick zum Themenfeld der Post-Privacy zu bieten. Die Forschungsfrage, die es zu klären gilt, lautet:

Welche gesellschaftlichen Chancen und Risiken ergeben sich aus einer aufkeimenden Transparenzkultur?

Methodisch (ohne hierbei standardisierte wissenschaftliche Signifikantien einzufordern) kann die Beantwortung dieser Frage nur anhand einer Diskussionsanlayse erfolgen. Wer schreibt über diese aufkeimende Kultur? Wer steht hinter ihr, vertritt sie und wer versucht ihre Verbreitung mit aller Vehemenz einzudämmen? Und warum? Welche Argumente messen sich im Für und Wider? Vor- und Nachteil, Chance und Risiko implizieren Wertungen wie „Gut und Schlecht" (Ergebnis) resp. „Gut und Böse" (Absicht). Ohne der Intention all zu wertend vorzugehen, stelle ich in dieser Arbeit nicht einfach willkürlich Argumente gegenüber und weise sie einer Schublade (gut oder böse) zu. Vielmehr werden hier die Wertungen aus den unterschiedlichen

Lagern gegenübergestellt. Was etwa für die DatenschützerInnen untragbar ist, kann für die Post-Privacy-VerfechterInnen einen gesellschaftlichen Nutzen bergen. Für die einen ein Nachteil, für die anderen ein Vorteil. Verkürzt: Wenn die einen (DatenschützerInnen) argumentieren, zu viel Transparenz mache das Individuum angreifbarer (Risiko), so kann dies für die andere Seite, also für das Lager der Post-Privacy-VertreterInnen, bedeuten, dass durch die kollektive Angreifbarkeit der Individuen, Hierarchien abgebaut werden (Chance). Geteiltes Leid. Die Nachteile bleiben also die altproklamierten. Die Vorteile, die als solche beworben werden, werden in jenen neuen Argumenten der Post-PrivatistInnen angeführt. Eine Gegenüberstellung und Dekonstruktion der IMHO wichtigsten Meinungen erfolgt in Kapitel 4.

Im übrigen gliedert sich die Arbeit in eine Klärung und geschichtliche Aufarbeitung des Privacy-Begriffs (Kapitel 1), die Absteckung der gesellschaftlichen Rahmenbedingungen (Kapitel 2) sowie die Präsentation des Forschungsstands und die Vorstellung der Post-Privacy Akteurinnen (Kapitel 3). Da die Beantwortung der Forschungsfrage bereits im 4. Kapitel erfolgt, leiste ich im letzten Kapitel einen reflektierenden Über- und Ausblick auf mögliche Entwicklungen der Post-Privacy.

Im ersten Kapitel erläutere ich nun, inwieweit sich das Verständnis des Begriffes und Wertes Privatsphäre über das letzte Jahrtausend verändert hat und was Post-Privacy überhaupt bedeutet.

1 Von der Privacy zur Post-Privacy

> Wir haben es mit der paradoxen Situation zu tun, dass [...] auf der einen Seite beklagt wird, dass Menschen überhaupt kein Interesse mehr an ihrer Privatsphäre haben, [...] auf der anderen Seite aber im selben Atemzug unterstellt wird, die Menschen hätten ein so starkes Interesse an ihrer Privatheit, dass [...] ihre informationelle Privatheit permanent verletzt wird oder jedenfalls bedroht ist. (Rössler 2001: 15)

Bevor ich den relativ neuen Terminus der Post-Privacy genauer besehe, gebe ich zunächst eine kleine geschichtliche Einführung in die Genese des Privaten. Ich versuche weiter zu erläutern, was gemeinhin unter Privatsphäre oder Privatheit verstanden wird und welche Erklärungsansätze es gibt. Die Begriffe Privatsphäre, Privatheit und Privacy sind dabei immer synonym zu verstehen. Außerdem nehme ich eine Begriffsdekonstruktion vor und erläutere warum für die vorliegende Arbeit insbesondere die sogenannte informationelle Privatheit, auf welche ich weiter unten eingehen werde, von Interesse ist.

In einem weiteren Unterkapitel suche ich nach den Ursprüngen des modernen Privacy-Begriffes, welchem ein juristisch-pragmatischer Ansatz zu Grunde liegt. Außerdem zeige ich mögliche erste Schnittstellen zwischen klassischen Konzepten der Privatsphäre und dem relativ neuen und wissenschaftlich kaum beachteten Feld der Post-Privacy auf. Sodann starte ich den Versuch einer ersten Definition des Terminus Post-Privacy, wobei festgehalten werden muss, dass diese Definition im Zuge der darauffolgenden Kapitel um zusätzliche Ebenen erweitert wird.

Vorweg muss ich ebenso festhalten, dass der Begriff Privatsphäre ein sehr vielschichtiger ist. Manch einer hat sich am Versuch einer Definition schon die Zähne ausgebissen: „Privacy seems to encompass everything, and there-

fore it appears to be nothing in itself." (Solove 2008: 7) Um den Begriff kreisen tatsächlich unterschiedlichste, teils widersprüchliche und gegeneinander konkurrierende Ansätze, dass es auch mir manchmal nahezu unmöglich schien, adäquat an den Begriff heranzutreten. Wie so oft, lohnt aber auch hier zunächst ein Blick in den Rückspiegel.

1.1 Geschichtsunterricht

‚Nur wer die Vergangenheit kennt, hat eine Zukunft' hat Wilhelm von Humboldt einmal gesagt. Der Fokus auf die Geschichte, verschafft uns also nicht nur einen besseren Überblick im Hier und Jetzt, er hilft uns möglicherweise auch dabei, uns auf das was noch kommt, vorzubereiten. Im Hinblick auf die Privatsphäre lernen wir aus diesem Axiom, dass uns die Geschichte, sofern wir nicht aufpassen, auch einholen kann. Das mag vielleicht noch etwas schleierhaft anmuten. Ich werde weiter unten (Kapitel 4.2.c), bezugnehmend auf einige dystopische Zukunftsprognosen , aber noch konkreter darauf eingehen.

Wie die meisten Begriffe stammt der Terminus 'Privat' aus dem Lateinischen und geht auf das Verb privare = berauben (Duden 2012: online) zurück. Führt man diesen Definitionsstrang fort, so wird aus dem privatus der/die Beraubte, der/die Abgesonderte oder der für sich stehende und nicht öffentliche Mensch (vgl. Duden 2012: online). In dieser negativen Konnotation lässt die Definition den Vergleich mit einem/einer EremitIn oder Sonderling der/die um seine/ihre Öffentlichkeit beraubt wurde, zu.

Privare bedeutet aber auch befreien (vgl. Duden 2012: online). Somit wird das Definitionsspektrum um wieder eine Ebene erweitert, und zwar um jene der

Freiheit als Wert. Eben jene Freiheit (des Individuums) wird im aktuellen Datenschutz-Diskurs auch immer wieder als unumstößliches gesellschaftliches Gut und Recht gehandelt, welches ein gewisses Maß an Privatsphäre voraussetzt und dadurch eng mit dieser verknüpft ist. Doch zurück zur Geschichte.

1.1a Antike

In der Antike, insbesondere im alten Rom war Privatsphäre, wie man sie heute kennt, kein gesellschaftlich hoch angesehener Wert. Es ging nicht darum sich von der Außenwelt abzuschotten um am Ende des Tages in den eigenen vier Wänden seine/ihre Ruhe zu finden. Das wäre auch gar nicht möglich gewesen, da das eigene Heim, sofern man ein gewisses Ansehen genoss, von dutzenden sog. Freigelassenen, Klienten, Sklaven und - nicht zu vergessen - den eigenen Familienmitgliedern, belagert wurde (vgl. Veyne 1989: 96). Alles Leben spielte sich nach Möglichkeit in, oder besser noch, im Sinne der Öffentlichkeit ab. Privatsphäre nach einem moderneren Verständnis, war nicht erstrebenswert und zeugte eher von der Unprivilegiertheit der breiten und niederen Masse (vgl. Heller 2012: 428). Der wahre Wert eines Mannes bewies sich im öffentlichen Ansehen,

> im Dienst an Rom, durch das Bekleiden staatlicher Ämter, bei glanzvollen Reden im Senat. Den eigenen Namen voranzubringen hieß zum Beispiel, öffentliche Bauwerke zu stiften. Sich groß zu machen hieß, möglichst viel vom eigenen Leben, Können, Reichtum in dieses gemeinsame Projekt der res publica zu stecken. (Heller 2012: 409)

Diese Praktiken der Selbstpräsentation zur Steigerung des Ansehens in der Öffentlichkeit, kann man durchaus auch als gesellschaftlichen Zwang sehen, der allerdings nur einer wohlhabenden Elite auferlegt wurde. „Die Reichen

waren genötigt, immer zu tun, was sie im Interesse ihres gesellschaftlichen Ranges gelegentlich getan hatten. Mit ihrer Großzügigkeit bezeugten die Notabeln, dass sie zur herrschenden Klasse gehörten." (Veyne 1989: 113)

Die res publica, die öffentliche Sache, erscheint in diesem Licht wie ein antikes Social Network. Zwar mit deutlich weniger Mitgliedern, aber funktionierend, nach den selben Faktoren einer „Aufmerksamkeitsökonomie" wie wir sie heute kennen. Nach dem Grundsatz: Wer nicht auffällt, fällt durch.

1.1b Mittelalter

Wie wir aus Geschichtsbüchern wissen, wurde dem römischen Reich das Leben im Überschwang und seine schiere Größe zum Verhängnis. Während es im Kern an seiner zunehmenden Fragmentiertheit scheiterte, so zerfranste es außen an den Zuströmen der Völkerwanderung. Die res publica wurde immer mehr zu res privata. Wo früher noch alles im Zeichen und Dienste der Öffentlichkeit geschah, herrschte plötzlich allgemeiner Rückzug und Abschottung. „Als die Sicherheiten des gemeinsamen politischen Gebildes unter Raubzügen und Wirtschaftskollaps wegfielen, sicherte sich eben jeder den Flecken Erde, auf dem er gerade saß, und zog drumherum einen Zaun gegen die nicht mehr ganz so verlässliche Umwelt." (Heller 2012: 483)

Die Zeit der feudalen Revolution war hereingebrochen und, was die damit verbundene Privatisierung der Macht betrifft, so ging mit ihr auch ein Paradoxon einher. Die aufgrund der Zersplitterung des Großreichs gebildeten mittelalterlichen Gemeinden waren klein und abgeschottet, und verstrahlten durch ihre Abgrenzung und Einhegung mit Hecken, Zäunen (vgl. Duby 1990: 26) und sonstigem Abgrenzungsallerelei ein hohes Maß an Privatheit. Doch

so privat sie nach außen hin auch erscheinen mochten, so wenig privat waren sie in ihrem Inneren. Der Lebenszusammenhang der die BewohnerInnen quasi umgrenzte, schuf ein vertrautes Milieu (vgl. Ariès 1985: 7). „In den Dörfern, in den Burgen, in den Klöstern kannte und überwachte ständig jeder jeden." (Heller 2012: 496). Dieser innere Verlust der Privatsphäre des/der Einzelnen war der Preis für den Schutz der Gemeinschaft.

Privatsphäre kann man im Mittelalter höchstens in einer Metaebene verorten, die nur für die sich voneinander abschottenden Gemeinschaften gilt. Privatsphäre im engeren Sinne wurde zwar zunehmend gefordert, war aber im engen Muff der Gemeinschaften schwer zu erlangen. Ganz für sich alleine sein oder sich mit der geheimen Liebschaft zu treffen, war am ehesten draußen in der Natur, vor den Mauern der Gemeinschaft und im Verborgenen möglich, in jenen „Leerzonen und Freiräumen [...] die der Intimität einen zwar unsicheren, aber bekannten und mehr oder weniger respektierten Schlupfwinkel boten." (Ariès 1986: 7)

Man muss allerdings hervorheben, dass es, wie in jedem Zeitalter, auch im Mittelalter resp. Feudalzeitalter unterschiedliche Ausprägungen von gelebter Privatsphäre gab. Während Familien aus ärmeren Schichten, ja teilweise heute noch, auf engstem Raum zusammengepfercht lebten und leben, ohne auch nur den leisesten Anspruch auf persönlichen Raum und Privatsphäre zu erheben, so wuchs bereits im Feudalzeitalter, zumindest in der gesellschaftlichen Elite, das Interesse an Intimität und persönlicher Sphäre enorm (vgl. Roncière 1985: 210). Bei der Lektüre dieser Zeilen zur Privatsphäre auf den unterschiedlichen Ebenen im Mittelalter (Abschottung von der Masse=Metaprivatsphäre vs. Verlust der Privatsphäre innerhalb der Gruppe=Mikroprivatsphäre), eröffnete sich mir ein interessanter Gedankengang. Wenn heute, in der Welt der Social Networks, ein junges Mädchen, das (möglicher-

weise etwas zu) behütet im Kreis der Familie aufwächst, nach Privatsphäre (im Sinne von Rückzug) sucht, so kann es diesen ‚Ort' möglicherweise im Netz und den Social Networks finden.

Es klingt paradox, wenn sich das Mädchen dazu entscheidet, Privatsphäre mit Öffentlichkeit zu vermischen um im Netz einen neuen Hort des Privaten zu schaffen. Noch paradoxer klingt es, wenn das Mädchen, die Freundschaftsanfrage der Eltern im Social Network ablehnt, um ihre dislozierte Privatsphäre zu schützen. Der Umgang mit Privatsphäre im Kontext einer neuen und ubiquitären Technologie, wie sie das Social Web mit all seinen Tools und Services darstellt, ist eben noch in einem frühen Stadium. „We're all experimenting and discovering our limits of privacy and publicness." (Jarvis 2011: 1826). Und nun wieder zur Geschichte.

1.1c Renaissance bis Biedermeier

Wie war es um die Privatheit in der Gesellschaft nach dem Mittelalter und Feudalzeitalter bestimmt? Ariès vermutet, dass es in der Zeit vom Spätmittelalter bis zum Ende des 17. Jahrhunderts keinen wirklichen Wandel der fundamentalen Mentalitäten gegeben hatte, so auch keinen was das Verständnis resp. das Ausleben von Privatsphäre betrifft. Er verortet allerdings drei äußere politisch-kulturelle Einwirkungen, die letztendlich für einen Mentalitätenwandel in der Neuzeit ausschlaggebend waren. Das waren zum Einen das Eingreifen des Staates und der Justiz in die Sozialzusammenhänge, sowie die Alphabetisierung und zum anderen der zunehmende Einfluss von Religiosität. (Vgl. Ariès 1986: 9-10) Wie wirkten sich all diese Einflüsse auf das Verständnis von Privatheit aus? Das vermehrte Einwirken des Staates in gesellschaftliche Strukturen manifestierte sich etwa in diversen Ver-

boten. So stellte man beispielsweise das Duellieren unter Strafe und schaffte diverse Kleidungsvorschriften unter Adelskreisen. Zur Bändigung individueller Macht- und Ehransprüche griff der Staat in derart private Bereiche ein, dass sich daraus letztlich eine gesellschaftliche Umstrukturierung entwickelte. So hatten diese staatlichen Einmischungen in private Bereiche zur Folge, dass zwischen der höfischen (Oberschicht) und der niederen (Unterschicht) Gesellschaft eine neue, kritische Mittelschicht aufkeimte, in welcher ein ebenso neues Interesse an Privatheit entfacht wurde. Jene Privatheit fand sich „im kleinen Amts- und Klerikaladel und bei den mittleren Amtsträgern, die das ganz ungewohnte Vergnügen genossen, unter sich zu bleiben und nur mit einer kleinen (wie man damals sagte) société auserlesener Freunde zu verkehren." (Ariès 1986: 9)

Der nächste Antriebsmotor für eine zunehmende Privatisierung, die Alphabetisierung, förderte das sog. stille Lesen, also das Lesen für sich alleine, ohne lauten Vorleser und der damit verbundenen Flüchtigkeit des Gehörten. Heller (vgl. 2012: 521) sieht darin die Genese einer Kultur der Innerlichkeit. „Der Leser konnte innehalten und nachdenken, die Sätze in seinem Kopf hin und her wenden, antworten und fragen." (ebd. 2012: 527) So hatte die Alphabetisierung und mit ihr der Trend zum stillen und einsamen Lesen auch zur Folge, „dass mancher sich sein eigenes Bild von der Welt machen und empirische Kenntnisse erwerben konnte. […] Es erlaubte die Reflexion, die sonst nur dem frommen Mann im Kloster oder in der Einsiedelei möglich war." (Ariès 1986: 10) So könnte man diese frühe Form des privaten, für sich Lesens auch als eine Vorstufe der modernen Individualisierung (Kapitel 2) deuten. Durch die Beschäftigung mit dem Text, der immer wieder neu erkundet werden kann, entsteht eine Beschäftigung mit sich selbst. Eine neue Form der Innerlichkeit brachte schließlich auch die voranschreitende Religiösität hervor, mit neuen Praktiken zur Erforschung des eigenen Gewissens, wie

etwa dem Gebet, der Beichte oder dem Tagebuch. Analog zur Entdeckung neuer Formen der Privatheit, lässt sich nach dem Feudalzeitalter auch die Entdeckung des Selbst beobachten. Galt es vorher noch „den Schein, d. h. die Ehre, also das eigene Gesicht zu wahren" (Ariès 1986: 9), so wurde plötzlich der Kern, das Innere interessant. „Der Einzelne horchte stärker in sich hinein, entdeckte sich dort als Ich und Eigenes." (Heller 2013: 527)

Eine neue Innerlichkeit fand man zu dieser Zeit auch in der eigenen Familie, welche zunehmend zum organisatorischen Zentrum des sozialen Raums wurde (vgl. Ariès 1986: 15). „Weg von einer eher nüchternen Einheit des Wirtschaftens und der Versorgung mit dem Notwendigen, hin zu einem Schutz und Liebeskörper um und für das aufzuziehende Kind" (Heller 2012: 539), vollzog sich die Familie bis ins 19. Jahrhundert hinein einem enormen Wandel. Die Familie und das eigene Heim wurden zum Refugium, in welchem die „Furcht vor dem bösen Blick" (Heller 2012: 590) regierte. Das bunte Gewimmel im eigenen Haus, so wie man es aus der Antike kannte, gehörte längst der Vergangenheit an. „Die Familie selbst schrumpfte auf Vater, Mutter und deren Kinder, in möglichst niedriger Zahl. Die Dienerschaft wurde in ihrer Zahl aufs Nötigste reduziert, in einen eigenen Trakt abgeschoben und nur noch bei Bedarf über Klingelzeichen hinzugeholt." (Heller 2012: 560)

Auch die pragmatische und unprivate Einrichtung des Hauses aus dem Feudalzeitalter, wich einer Individualisierung und Privatisierung. Auch wenn das Private im Grunde immer noch zum Bereich des Gedachten und Geheimen gehörte, so gab es nun zumindest Orte an denen man diesen Gedanken ungestört folgen konnte. So manifestierte sich die Privatisierung auch in der Ausdifferenzierung der Räume. Aus Mehrzweckhallen wurden nun voneinander abgetrennte Zimmer, in die man eintreten und alsdann die Tür hinter sich schließen konnte (vgl. Ranum 1986: 216). Das traute Heim wurde so

zum Hort, zur privaten Bastion gegen die harte und schonungslose Welt draußen, die Öffentlichkeit.

Die strikte Trennung zwischen jenen privaten, familiären Sphären und der Öffentlichkeit zur Zeit um die französische Revolution, lässt sich auch analog zu einer Geschlechtertrennung zwischen Mann und Frau aufzeigen. Auf der einen Seite stand der Mann der sich täglich dem Geschäft, der Politik, den öffentlichen Belangen widmen musste, auf der anderen Seite die Frau, welche zusammen mit den Kindern im Privaten abgekoppelt wurde. „Ehefrau und Mutter zu sein war der Beruf der Frau, Heim und Herd ihr Einflussbereich und Ort ihres Handelns. Die weiträumige Bühne öffentlicher Betätigung blieb ihr verschlossen. Sie konnte ihren Stern im Haus erstrahlen lassen, im Schatten des Ehemannes." (Hall 1987: 61)[2]

1.1d Biedermeier

Im 19. Jahrhundert schließlich erreichte die Einmottung der Familie ins Private ihren vorläufigen Höhepunkt. Stärker als je zuvor grenzte man sich in der eigenen privaten Sphäre gegen das Getose der Außenwelt ab und „so erfand sich das Biedermeier als Erholung von Napoleon und das englische Landhaus als Gegenentwurf zur rumorenden Stadt." (Heller 2012: 590) In Frankreich leistete der Staat dieser familiären Abschottung rechtlich Vorschub, indem er etwa die nächtlichen Hausdurchsuchungen abschaffte und die Wohnung für unantastbar erklärte. (Vgl. Perrot 1987: 421)

---

[2] Hier sei angemerkt, dass ich für ein ordentliches Verständnis des Begriffes Privatsphäre, eine solche Geschlechterteilung als überwunden ansehe. Dieser traditionellen Auffassung, welche im grundsätzlichen Widerspruch einer liberal-demokratischen Grundhaltung steht, ziehe ich einen geschlechtsneutral notierten Begriff vor. Dabei beziehe ich mich auf die „Idee von Privatheit als einer Norm, die für alle Personen in gleicher Weise zu gelten hat, und nicht für Frauen und Männer in je verschiedener Weise." (Rössler 2001: 18)

Doch was war da draußen? Was war das Böse, vor dem es die Familie, die Kinder, die Frauen zu Hause zu schützen galt? Da waren die neuen Technologien wie die Fotografie, die nicht nur das eigene Abbild, ja vielleicht sogar die eigene Persönlichkeit abbildet. Dann gab es neue Informationsmethoden, welche etwa in Form der Klatschpresse ganz neuartige Probleme aufwarfen. „Die Presse war begierig auf Vermischtes, das heißt: auf enthüllende Skandale aus der Privatsphäre." (Perrot 1987: 421) Man musste sich geradezu verstecken oder zumindest verstellen, in diesem „neugierigen Jahrhundert" (Perrot 1987: 422), um nicht negativ aufzufallen. Geistig behinderte Familienangehörige wurden weggesperrt, dunkle Familiengeheimnisse vergraben, damit ja nichts unrühmliches an die neue Öffentlichkeit drang. Selber freilich, ergötzte man sich an den Bescholtenheiten der anderen und bediente sich dabei eben jener Klatschblätter oder besuchte die psychiatrischen Zurschaustellungen der HysterikerInnen (vgl. Heller 2012: 599).

Das Biedermeier war das Zeitalter der Familie und deren Schutz. Staatliche Institutionen waren sich im Klaren, Familien seien der Grundpfeiler, „die unsichtbare Hand einer funktionierenden Gesellschaft und der verborgene Gott der Ökonomie." (Perrot 1987: 122) Aller Schutz galt diesem Hort der Moral und der Sitte, ohne welchen die Gesellschaft nur aus wahllos zusammengewürfelten Gruppen bestünde, „die für jeden beliebigen Despotismus anfällig sind." (Perrot 1987: 100)

So war das Biedermeier auch das Zeitalter der Privatsphäre. Allerdings hat der Begriff, zumindest aus heutiger Sicht, eine stark räumliche und immer noch geschlechterspezifische Konnotation. Privatsphäre definierte damals eine Sphäre, die ganz und gar häuslich ist, klar von der Öffentlichkeit abgeschnitten, durch dicke, schützende Trennwände. Draußen die harte Welt der

Politik, der Krieg, kurz die Öffentlichkeit, die von den Männern dominiert wurde. Und drinnen das Weibliche, das Private. Die Familie war der Kompensator und gleichzeitig Fundament für das Draußen. Sie war der „Schlüssel zu privatem Glück und öffentlichem Wohl." (Perrot 1987: 104).

Was so essenziell für das Funktionieren der Gesellschaft war, wollte auch rechtlich zementiert sein. So kamen schließlich zwei junge Rechtsanwälte auf den Plan, den Hort des Privaten und dessen Unantastbarkeit in einen Rechtsrahmen zu zwängen. Der Wert des Privaten musste geschützt werden.

1.2 Das Recht auf Privatsphäre

Wer sich heute im Netz umsieht um nach klassischen Privacy-Konzepten zu suchen, der/die stößt ziemlich schnell auf das Schriftstück „The Right to Privacy" (Warren/Brandeis 1890: online), verfasst von den Rechtsanwälten Samuel D. Warren und Louis D. Brandeis. Aus dem um die Wende vom 19. zum 20. Jahrhundert veröffentlichten Beitrag, lässt sich komprimiert etwa folgende Aussage extrahieren. Privacy is „the right to be let alone." (Warren/Brandeis 1890: online) Privatsphäre ist demnach das Recht darauf, alleine resp. in Ruhe gelassen zu werden, und zwar in einer Zeit in der Gossip und Yellow-Press zunehmend Verbreitung finden, in der Fotografien von Privatpersonen plötzlich in öffentlichen Zeitungen abgedruckt werden, in der, kurzum, neue gesellschaftsrelevante Technologien etabliert werden. Vor diesem Hintergrund wirkt das Schreiben wie ein Pamphlet, ein Aufschrei inmitten des nicht mehr zeitgemäßen Gesetzesdschungels. „solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury." (1890: 3)

Warren und Brandeis erging es wohl nicht anders, als vielen DatenschützerInnen heutzutage. Auch sie sahen sich mit einer schier unüberschaubaren Technologien- und Informationsvielfalt und den daraus resultierenden Gefahren konfrontiert und versuchten die BürgerInnen und GesetzgeberInnen gleichermaßen dafür zu sensibilisieren.

TransparenzverfechterInnen sehen heute in diesem Verhalten oft eine übertriebene Angst vor neuen Technologien. „Technology [...] breeds fear. Again and again in history, technology has caused change and that change has

sparked worries that privacy is being threatened or that publicness is being thrust upon us." (Jarvis 2001: 217) Um das Prinzip von Warrens und Brandeis' früher Auffassung von Privatsphäre zu verdeutlichen, können wir sie als Schablone auf heutige gesellschaftliche Phänomene legen. Aus heutiger Sicht mag das Recht in Ruhe gelassen zu werden, staubig und überholt wirken. Wie soll das gehen? Fragt man sich etwa im Angesicht von Facebook, einem omnipräsenten soziotechnischen Phänomen, das auf Dauerinteraktion und der Öffentlichmachung von privaten Informationen aufbaut und mehr oder weniger freiwillig von einem Siebtel der Menschheit genutzt wird (vgl. Facebook Newsroom: online). Ob das noch zeitgemäß ist, ob das überhaupt gewollt ist, darüber zerbrechen sich DatenschützerInnen und insbesondere DatenschutzgegnerInnen die Köpfe.

Dem Recht, in Ruhe gelassen zu werden, liegt ein sehr defensives Prinzip - im Sinne von Verteidigung - zu Grunde. Es gilt die Privatsphäre zu verteidigen, zu schützen, dem Individuum das Recht einzuräumen, persönliche Informationen geheim zu halten. Schlüsselfaktor ist dabei aber nicht etwa nur das Eigentumsrecht, also die Besitzhoheit über die persönlichen Informationen und Daten, sondern die Persönlichkeit selbst. Anders formuliert: Persönliche Informationen über ein Individuum müssen nicht deswegen geschützt werden, weil sie dessen geistiges Eigentum darstellen, sondern weil sie dessen Persönlichkeit betreffen, welche wiederum unantastbar bleiben muss. „The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality." (Warren/Brandeis 1890: 7) Der Schutz der Privatsphäre dient hier also einem scheinbar höherem Ziel: Dem Schutz der Persönlichkeit. Dieses Argument ist gleichzeitig auch gutes Kanonenfutter für eine Einforderung des Rechts auf informationelle Selbstbestimmung.

1.3 Privatsphäre und Selbstbestimmung

Aus der frühen Privacy-Definition (The right to be let alone) von Warren und Brandeis lässt sich auch das heute von vielen DatenschützerInnen geforderte - und in Deutschland gesetzlich verankerte - Recht auf informationelle Selbstbestimmung ableiten, auch wenn es nicht direkt darauf beruht, sondern auf ein etwas moderneres Konzept zurückgeht. Alan F. Westin etwa bricht in seinem Beitrag „Privacy and Freedom" (1970) seine Vorstellung von Privatsphäre auf ein dezidiertes Recht des/der Einzelnen herunter, über die Verbreitung der die eigene Person betreffenden Informationen zu bestimmen. Demnach sei Privatsphäre „the right of the individual to decide what information about himself should be communicated to others and under what circumstances." (Westin 1970: o.S.)

Warrens und Brandeis' defensives Konzept weicht hier einem offeneren Ansatz. Auch die weiter unten (Kapitel 1.4) erwähnte Idee der informationellen Privatheit von Rössler (2001) schlägt in diese Kerbe. Nach wie vor gilt es das Private zu schützen, gleichwohl wird aber auch die Option der Offensive mit eingeräumt. Es heißt nun: Du musst zwar nichts preisgeben, darfst aber. Und wir - das Gesetz - schaffen den gesetzlichen Rahmen dafür. Eben jener Rahmen wurde etwa schon in Deutschland geschaffen und geht aus dem gesetzlich verankerten Schutz des Persönlichkeitsrechts hervor: eben das Recht auf informationelle Selbstbestimmung.

> Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf 'informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig. (Virtuelles Datenschutzbüro: online)

Das 1983 nach einem Volkszählungsurteil anerkannte Grundrecht scheint vor allem aus einer Notgedrungenheit im Kontext des neuen, explodierenden Wirtschaftszweigs der elektronischen Datenverarbeitung entsprungen zu sein. Es gehe nämlich um den „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten." (Virtuelles Datenschutzbüro: online) Privatsphäre wird vor diesem Hintergrund zu einem Konglomerat aus persönlichen Informationen und vor allem persönlicher Daten.

Problematisch ist die Einforderung des Grundrechts aus vielerlei Hinsicht. Die Krux findet sich bereits in der Formulierung des Satzes. Demnach seien Einschränkungen des Rechts auf informationelle Selbstbestimmung, wie erwähnt, nur im überwiegenden Allgemeininteresse zulässig. Wie dehnbar diese Auslegung ist, verdeutlichen viele gesetzliche Errungenschaften der letzten Jahre von Vorratsdatenspeicherung bis ACTA (vgl. Electronic Frontier Foundation 2012: online). So mokieren sich etwa Constanze Kurz und Frank Rieger vom Chaos Computer Club an der „raumgreifenden Speichergier des Staates" (Kurz/Rieger 2011: 10), im Zuge derer nahezu flächendeckend, das Kommunikationsverhalten der Bevölkerung gespeichert wird, „mit der vagen Begründung, dass man die Daten ja eventuell mal zur Strafverfolgung benötigen könnte." (Kurz/Rieger 2011: 10)

Lücken im Recht zur informationellen Selbstbestimmung sieht selbst der deutsche Bundesbeauftragte für Datenschutz und Informationsfreiheit Peter Schaar. Auf seiner Website lässt sich der Nachholbedarf herauslesen: „Wie soll das Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen Datenverarbeitung ausgestaltet sein? Das heutige Datenschutzrecht gibt hierauf nur noch unbefriedigende Antworten und bedarf der Modernisierung." (BFDI 2012: online) Die Frage könnte auch lauten - und

damit wird die nächste Crux deutlich - Wie soll das Recht auf informationelle Selbstbestimmung im Zeitalter der zunehmenden freiwilligen Datenveräußerung ausgestaltet sein? Anders und radikaler formuliert: Wie soll man das Recht auf Privatsphäre oder das Recht zur informationellen Selbstbestimmung durchsetzen, wenn es weitläufig nicht einmal mehr reflektiert resp. gefordert wird? Und damit sind wir beim Gegenentwurf angelangt: Der Post-Privacy-Debatte.

Insgesamt lässt sich zusammenfassen, dass der Begriff Privatsphäre im aktuellen Diskurs häufig im juristischen Kontext benutzt wird. Wir sprechen vom Schutz der Privatsphäre und vom unumstößlichen Recht auf Privatsphäre. Dem Recht zum Schutz der eigenen Daten und persönlichen Informationen. Aber auch dem Recht zur Hoheit, zur Kontrolle über selbige und der damit verbunden Freiheit darüber zu bestimmen, was von den persönlichen Informationen und Daten nach außen dringen darf und was nicht.

1.4 Die drei Dimensionen des Privaten

Ich frage erneut. Was meinen wir, wenn wir das Wort Privatsphäre in den Mund nehmen? Einen gesellschaftlichen, philosophischen oder einen juristischen Wert, einen metaphorischen oder tatsächlichen Raum? Wie schon erwähnt, gibt es etliche Zugänge zum Begriff Privatsphäre, die sich gegenseitig aber nicht immer zwingend ausschließen müssen. In der aktuellen Diskussion zum Schutz der Privatsphäre werden all diese genannten Ebenen tatsächlich auch vereint. Privatsphäre gilt nicht nur unter DatenschützerInnen als hart erkämpftes und schützenswertes gesellschaftliches Gut. Sie stellt gleichzeitig einen Raum dar, der sich vom öffentlichen Raum mehr oder weniger abgrenzen lässt und ist gesetzlich fest verankert. Privatsphäre ist also

durchaus ein mehrdimensionaler Begriff. Nach Beate Rössler ein dreidimensionaler.

> Geht es um Daten über eine Person, also generell darum, was andere über mich wissen, dann geht es um meine informationelle Privatheit. Geht es um meine privaten Entscheidungen und Handlungen (mit wem will ich zusammenleben; welchen Beruf will ich ergreifen; aber auch: welche Kleidung trage ich), dann geht es um meine dezisionale Privatheit; und steht die Privatheit meiner Wohnung zur Debatte, dann rede ich von lokaler Privatheit. (Rössler 2001: 17)

Darüber hinaus sei Privatheit, ganz egal in welchem dieser drei Kontexte, immer im engen Schulterschluss mit Kontrolle zu sehen. Das Individuum das also von Privatheit spricht und selbige einfordert, fordert gleichzeitig auch Kontrolle über den Zugang zur besagten Privatheit (vgl. Rössler 2001: 16). Im konkreten Falle der informationellen Privatheit leistet Rössler hier auch einem - unter DatenschützerInnen immer wieder heiß diskutierten - Thema Vorschub, und zwar der informationellen Selbstbestimmung. Wie bei der informationellen Selbstbestimmung geht es auch bei der informationellen Privatheit „darum, wer was wie über eine Person weiß, also um die Kontrolle über Informationen, die sie betreffen." (Rössler 2001: 20) An diesem Gegenstand äußern sich die stärksten Kontrastpunkte zwischen Privacy- und Post-Privacy-VerfechterInnen. Deshalb lege ich in der vorliegenden Arbeit das Hauptaugenmerk auch auf eben jene informationelle Privatheit und meine mit Post-Privacy demnach auch vorwiegend die post-informational-privacy.

1.5 Privatsphäre und Freiheit

> The free man, is the private man. (Rossiter/Konvitz 1957: 15)

> Sonst leben wir in unseren durchsichtigen, wie aus leuchtender Luft gewebten Häusern, ewig vom Licht umflutet. Wir haben nichts voreinander zu verbergen. […] Die sonderbaren, undurchsichtigen Behausungen unserer Vorfahren können es bewirkt haben, dass man auf diese erbärmliche Käfigpsychologie verfiel: 'Mein Heim ist meine Burg.' (Samjatin 1977: 31)

My home is my castle. Das klingt zunächst tatsächlich wie ein Paradoxon. Was soll der Wert Freiheit mit dem Wert Privatsphäre zu tun haben, fragen sich die wenigen Bewohner des ‚Einzigen Staates' aus Samjatins Zukunftsroman? Wer sucht seine/ihre Freiheit schon im Rückzug? Was sind die eigenen vier Wände oder der eigene Kokon[3] schon gegen das Draußen, die Weite oder gemeinhin, Freiheit?

Der Widerspruch hält natürlich nicht, zumal es sich beim Terminus Freiheit im vorliegenden Kontext um einen Wert handelt, der sich nicht in einer bestimmten räumlichen Fläche oder einem Volumen ausdrücken lässt. Freiheit heißt „die Freiheit des Einzelnen […] in einer liberal-individualistischen Gesellschaft." (Heller 2013: 675) Der Wert umfasst die Freiheit selbst über etwas bestimmtes zu entscheiden oder etwas zu kontrollieren. Im Zusammenhang mit Privatsphäre heißt dies: Wer den Zugang zu seinem/ihrem privaten Leben nicht kontrollieren kann, wer nicht darüber entscheiden kann, welche Bereiche seines/ihres Lebens an die Öffentlichkeit gelangen, der/die ist unfrei. Doch schauen wir noch einmal zurück. Woher rührt die strikte Verbindung dieser zwei Werte?

---

[3] erwähnenswert ist in diesem Kontext das Cocooning (vgl. Popcorn 2013: online). Es beschreibt einen gesellschaftlichen Trend, den man durchaus mit der forcierten Häuslichkeit des Biedermeier vergleichen kann. Dabei geht es um den Rückzug ins eigene Heim, zum Schutz vor der gefährlichen und krisengebeutelten Außenwelt. Im Biedermeier erholte man sich von den Strapazen der Revolution, heute versteckt man sich vor den omnipräsenten Krisen und Gefahren der Welt.

Ein erster Zusammenhang lässt sich vermutlich wieder im historischen Kontext beim Historiker Philippes Ariès verorten. In seinem fünfteiligen und mehrere tausend Seiten umfassenden Beitrag zur Geschichte des privaten Lebens, kam er unter anderem zum Schluss, dass Privatheit und Öffentlichkeit sehr stark mit Herrschaftsstrukturen zusammenhängen. Öffentlich oder Öffentlichkeit hat etwas mit Staat und Staatsdienst zu tun, wonach sich Privatheit klar vom öffentlichen Machtgefüge abgrenzt und eben das bezeichnet, was sich „jenseits der staatlichen Herrschaft abspielt." (Ariès 1986: 17) Individuelle Privatheit, so könnte man nun interpretieren, findet sich also nur in jenen Lebensbereichen, die sich von staatlichen und institutionellen Machteinflüssen emanzipiert haben. Dies kann in den eigenen vier Wänden sein, im Brief, in der E-Mail. Diese privaten Räume zu definieren und vor allem zu schützen ist wiederum Aufgabe des Staates.

Privatheit unterstützt also eine gewisse Form von Freiheit, sowohl die Freiheit von Einflüssen oder Einblicken des Staates oder einer übergeordneten Macht, als auch die Freiheit selbst darüber entscheiden resp. kontrollieren zu können, wer oder was in diese Privatheit eindringen darf und was nicht. Historisch betrachtet, wurde das Bündnis zwischen Freiheit und Privatsphäre, durch die Abgrenzung von stalinistischen Überwachungskonzepten in Stasi-Manier gefestigt. Die dystopischen Romane von Orwell, Huxley und Samjatin, welche düstere Szenarien totalitärer Überwachungsgesellschaften zeichnen, dienten dabei stets als Kanonenfutter im Sinne liberaler Konzepte, welche die Privatsphäre zunehmend als schützenswerte Bastion erachteten. So wurde die Privatsphäre zur Agentin der Freiheit.

Heute zweifeln insbesondere die GegnerInnen eines zu vehement geforderten Datenschutzes an diesem als gemeinhin unumstößlich erachteten Zusammenhang zwischen Privatsphäre und Freiheit.

Sie verlangen nach anderen, zeitgemäßeren und zielgerichteteren Definitionen von Privatsphäre, welche den Konnex zur Freiheit in ein anderes Licht rücken. So echauffiert sich beispielsweise ein Mitglied der ‚Datenschutzkritischen Spackeria' auf einem Blog darüber, dass die aktuelle Diskussion um den Datenschutz und die Freiheit in die falsche Richtung ziele. „Was bei […] Definitionen von Privatsphäre auffällig ist, ist ihr Fokus auf Metainformationen über Menschen unter Vernachlässigung der Bedürfnisse des Menschen. Die Definitionen sprechen über Mechanismen, über einzelne 'Tools', die etwas spezielles erreichen oder garantieren sollen, ohne aber das eigentliche Ziel zu benennen." (Geuter 2011: online) Der Datenschutzkritiker sieht den Privacy-Begriff zwar auch im engen Schulterschluss mit Freiheit, allerdings aus einem völlig anderen Blickwinkel als dem der kritischen Datenschützer-Warte. Anhand von Agres' und Rotenbergs Ansatz, welcher Privatsphäre als „freedom from unreasonable constraints on the construction of one's own identity" (1998: 7) definiert, könnte man hier den Spieß umdrehen.

Nicht mehr die Privatsphäre oder der Datenschutz sind Agenten oder „Krücken" (Geuter 2011: online) der Freiheit, sondern umgekehrt. Anders formuliert: Das vehemente Einfordern des Datenschutzes oder des Schutzes der Privatsphäre muss nicht per se Freiheiten aufrechterhalten, sondern kann selbige auch beschneiden. Wer Beispielsweise Facebook, Google+ oder ähnliche Services nutzt, sei es um sich selbst gut darzustellen, sich zu vernetzen oder einfach nur Tagebuch zu führen der/die betreibt bereits Identitätskonstruktion und -konstitution. Beschneidet man durch den Datenschutz jene Tools, welche die Identitätskonstruktion fördern, so beschneidet man auch die Möglichkeit zur Entfaltung der eigenen Identität, so die Annahme der DatenschutzkritikerInnen mit Bezugnahme auf Agres und Rotenberg.

In eine ähnliche Kerbe schlägt die Aussage eines deutschen A-Bloggers, welchen ich im Zuge der Dreharbeiten unseres Masterprojekts Miio interviewt habe. Mario Sixtus treibt mit der Auffassung „Freiheit ist eigentlich nichts anderes als ein Mehr an Optionen als der Unfreie hat" (Sixtus 2011: Interview) einen Keil zwischen die Werte Privatsphäre und Freiheit. Entsprechend der Logik, dass der Datenschutz die Verbreitung und Nutzung bestimmter Technologien einschränken möchte, hieße das auch, nicht nur die mit eben diesen Technologien verbundenen Risiken abzuwehren, sondern auch auf die möglichen Freiheiten und Erleichterungen, welche sie hervorbringen können, zu verzichten.

Eine Trennung der Begriffe Freiheit und Privatsphäre findet man auch bei David Brin (1998). Er glaubte bereits vor 15 Jahre, also lange vor dem Aufkeimen des Web 2.0 und der daraus resultierenden Massensozialisierung des Internet, dass das rasante Fortschreiten technologischer Entwicklungen zwangsläufig dazu führen würde, dass sich die Gesellschaft irgendwann zwischen Privatsphäre und Freiheit entscheiden müsste. Als Untertitel für David Brins Beitrag „The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom?" ist diese strikte Spaltung zweier eigentlich untrennbarer Werte, durchaus provokant gewählt. Brin rudert sodann auch zurück. „It may be possible to have both liberty and some shelter from prying eyes. But suppose the future does present us with an absolute either-or decision, to select just one, at the cost of the other. In that case, there can be no hesitation." (Brin 1998: 13) Brin würde für die Freiheiten der Post-Privacy die Privatsphäre aufgeben. Einem/r DatenschützerIn würde es bei der Frage ‚Freiheit oder Privatsphäre?' wohl die Sprache verschlagen.

Es wird also deutlich, dass sich die beiden Begriffe Privatsphäre und Freiheit schwer unter einen Hut bringen lassen. Privatsphäre und Freiheit als un-

trennbare Einheit anzusehen, ist für eine sinnvolle Diskussion IMHO nicht gerade zielführend. Manchmal dient etwa der Datenschutz im Sinne der Privatsphäre als Agent der Freiheit. Ein andermal kann zu viel Datenschutz im Sinne der Privatsphäre bestimmte Freiheiten einschränken. Das Zwangsbündnis ist nicht per se zu legitimieren. Das Verhältnis muss von Fall zu Fall, immer wieder neu ausgehandelt werden. Ein banales Beispiel: Ein/e ArbeitgeberIn der/die bei der Auswahl seiner/ihrer MitarbeiterInnen nach potentiellen KandidatInnen und deren dunkler Vorgeschichte googelt, genießt die Vorteile und Freiheit der Technologie. Umgekehrt kann dies für den/die JobanwärterIn einen tiefen Einschnitt in die Privatsphäre und, daraus resultierend, auch einen ebenso tiefen Einschnitt in die Freiheit der Berufswahl bedeuten. Es kommt eben immer auf die Umstände an. Aussagen wie die des Vizepräsidenten der Europäischen Union Alexander Alvaro wirken daher nahezu illusorisch. „Nur weil wir neue Technologien haben, die uns das Leben erleichtern sollen, kann es nicht auf der anderen Seite bedeuten, dass wir dafür den Verlust anderer Freiheiten hinnehmen müssen." (Alvaro 2011: Interview) Neue Technologien schaffen gewiss neue Chancen, dafür bergen sie aber auch Risiken und können uns manche lieb gewonnene Freiheit wieder nehmen.

All diese weiter oben genannten Begriffsgegenüberstellungen, insbesondere jene der Privatsphäre und der Freiheit und dazu noch im historischen Vergleich, zeigen auf, wie unterschiedlich die Auffassungen sind und wie vielschichtig und vielseitig die einzelnen Begriffe gedeutet werden können. Die Werte Öffentlichkeit, Privatsphäre, Freiheit und deren Zusammenhänge haben im Laufe der Jahrhunderte einen enormen Wandel durchgemacht. Heute stehen auf der einen Seite die DatenschützerInnen, welche den hart erkämpften Grundwert der Privatsphäre um jeden Preis verteidigen möchten. Auf der anderen Seite keimt langsam eine offenere Gruppierung auf, welche

den Wert und Begriff Privatsphäre neu definieren, und den uneingeschränkten Schutz derselben, zum Teil aufheben möchte. Auf eben diese AkteurInnen einer neuen Offenheitskultur und ihre Vorstellungen zu einer transparenten Gesellschaft, gehe ich im dritten Kapitel ein.

Nach diesem Gros an Definitionen, welche fast ausnahmslos auf die Mannigfaltigkeit des Begriffs Privatsphäre verweisen, bleibt die Frage: Was ist eigentlich Post-Privacy?

1.6 Was ist Post-Privacy?

Das Präfix Post lässt bereits darauf schließen, dass mit Post-Privacy ein Leben nach der Privatsphäre gemeint ist. Das alte Modell der Privatsphäre gilt dabei als überwunden. Ihr Ende wird häufig recht theatralisch illustriert. Schuld ist immer das Internet:

> Conventional wisdom today is, of course, that privacy is dead. The internet wounded it. Facebook killed it. (Jarvis 2011: 1807)
>
> You have zero privacy anyway. Get over it. (Mc Neilly 1999: online)
>
> Unser Sein und Handeln, egal wie persönlich oder geheimniskrämerisch, ist zunehmend für andere einsehbar. Wir müssen lernen damit klarzukommen. (Heller 2012: 65)

Es ist kaum zu übersehen. Der Grundton dieser neuen „Transparenz-Theorie" (Kurz/Rieger 2011: 183) ist resignativ. Die Privatsphäre ist tot, dank Internet, Technologie, Überwachung etc. Man könne einfach nichts dagegen machen. Erst in der letzten Aussage, in diesem 'Lernen damit klarzukommen', im Lernen mit der neuen Situation umzugehen, liegt IMHO der Auftrag der Post-Privacy-Theorie. DatenschützerInnen haben sich die Verteidigung

der letzten Horte der Privatsphäre auf die Fahnen geheftet und fragen sich: Wie schützen wir die Privatsphäre vor staatlichen oder wirtschaftlichen BedrängerInnen? Post-PrivatistInnen konzentrieren sich auf das genaue und teils radikale Gegenteil und konstatieren: Datenschutz ist aussichtslos (vgl. Heller 2011: 1486). Wie also machen wir uns den Umstand der zunehmenden Transparenz zu Nutze? Sie gehen sogar noch einen Schritt weiter und fordern das Aufgeben der letzten Reste von Privatsphäre. Dies schaffe gesellschaftliche Chancen (siehe Kapitel 4). „Transparenz öffnet Anschlüsse für Solidarität, verschafft Reichweite und befördert die Kommunikation." (Heller 2012: 2205)

In ihrem Selbstverständnis der Überwindung einer Privatsphäre wie man sie bisher kannte und schützte, kann man die Begriffe Privacy und Post-Privacy auch anhand einer Definition der Moderne resp. Post-Moderne beschreiben. und nicht nur wegen ihres gemeinsamen Präfix'. Hierzu ziehe ich Zygmunt Baumans Definition der Postmoderne heran.

> Das ist es letztlich, wofür die Idee Postmoderne steht: eine Existenz, die völlig durch die Tatsache bestimmt und definiert ist, dass sie post ist (hinterher kommt) und überwältigt ist vom Bewusstsein, sich in einer solchen Lage zu befinden. Postmoderne bedeutet nicht notwendig das Ende, die Diskreditierung oder Verwerfung der Moderne. Postmoderne ist nicht mehr (aber auch nicht weniger) als der moderne Geist, der einen langen, aufmerksamen und nüchternen Blick auf sich selbst wirft, auf seine Lage und seine vergangenen Werke, nicht ganz überzeugt von dem, was er sieht, und den Drang zur Veränderung verspürt. Postmoderne ist die Moderne, die volljährig wird: die Moderne, die sich selbst aus der Distanz betrachtet statt von innen. [...] Postmodern ist die Moderne, die sich mit ihrer eigenen Unmöglichkeit abfindet; eine sich selbst kontrollierende Moderne, eine, die bewusst aufgibt, was sie einstmals unbewusst getan hat. (Bauman 1992: 333)

Tauscht man hier die Begriffe ‚Postmoderne' mit ‚Post-Privacy' und ‚Moderne' mit ‚Privatsphäre' aus, so ist Baumans Ansicht immer noch schlüssig. Post-Privacy ist zunächst einmal post (also hinterher), wie weiter oben be-

schrieben. Gewissermaßen ist sie auch ein Kind der Postmoderne. Getrieben von, resp. geboren aus dem Drang zur Veränderung, muss sie sich auch erst noch finden und ihre Postition behaupten. Post-Privacy muss auch nicht unbedingt das uneingeschränkte Aus resp. eine Diskreditierung für die Privatsphäre bedeuten.[4] Sie reflektiert sich gerade selbst und die gesellschaftlichen Umstände, aus welchen sie erwuchs und geht mit klassischen Privatsphäre-Konzepten und deren Schutzbeharren in die Kritik. Post-Privacy resp. jene AkteurInnen welche die Post-Privacy als Begriff festmachen wollen, stellen Gegebenes in Frage, kritisieren, dekonstruieren. Post-Privacy steht im Zeichen der Veränderung ohne sich bisweilen etabliert zu haben. Sie ist vieles: Postmodern, antimodern (vgl. Zeger 2008: 33) und - glaubt man ihren VerfechterInnen - nicht mehr aufzuhalten.

Nachdem nun die Begriffe, resp. deren Mannigfaltigkeit und Vielschichtigkeit, thematisiert wurden, gehe ich im folgenden Kapitel auf die gesellschaftlichen Rahmenbedingungen ein, die ein Aufkeimen der Post-Privacy-Kultur begünstigen.

[4] Gewisse Teile der Gesellschaft, bestimmte Geheimnisse und Gedankengänge ihrer Individuen werden immer privat bleiben und müssen je nach Kontext auch besonders geschützt zu werden. Man denke nur an DissidentInnen in repressiven Regimes oder Wikileaks-InformantInnen.

2 Entstehungskontext und Rahmenbedingungen

Im ersten Kapitel habe ich den Werdegang der Privatsphäre im Zuge der Epochen des vergangenen Jahrtausends zusammengefasst. Ich habe dargelegt, wie die Bedeutung dieses Begriffes, je nach Zeitalter und den herrschenden gesellschaftlichen Rahmenbedingungen, immer wieder neu ausgehandelt wurde. In diesem Kapitel gehe ich auf einige gesellschaftliche Metaprozesse ein, welche die Ausbreitung der Post-Privacy-Kultur in unserem Zeitalter begünstigen.

2.1 Individualisierung

Die Individualisierung, als Prozess des Ausbruchs des Individuums von der Fremd- zur Selbstbestimmung, geht stark mit den Übergangseffekten der Moderne zur Postmoderne einher. Die Postmoderne bezeichnet an dieser Stelle, in Abgrenzung zur Moderne, „gesamtgesellschaftliche Erscheinungen der Heterogenisierung, der Pluralisierung, der Werteverschiebungen sowie der Flexibilisierung und Individualisierung innerhalb der modernen Kultur." (Misoch 2004: 68)

Während die Moderne, diese „einheitliche Welt" (Abels 2006: 420), durch „relative Vorhersagbarkeit und soziale Absicherung" (Misoch 2004: 49) den Individuen noch Orientierung bot, löst sich diese im Wechsel zur Postmoderne mehr oder minder auf. Das Individuum wird gewissermaßen befreit, aus „traditionalen Herrschafts- und Versorgungszusammenhängen sowie traditionellen Interaktionsformen" (Krotz 2001: 241) wie man sie vorher etwa in der Familie oder im Schutz einer fest etablierten Privatsphäre fand.

Abgesehen vom teilweisen Verlust des alten Orientierungswissen, „also traditional begründetem Handlungswissen, Glauben, Normen" (Krotz 2001: 241), bringt die Individualisierung den Menschen aber auch ganz neue Freiheiten. Einmal befreit aus dem Muff der festgefahrenen Moderne, ist das Individuum stets offen und flexibel für das „was der Zeitgeist bietet und gebietet." (Abels 2006: 418).

Betrachtet man die Individualisierung als noch nicht abgeschlossenen Prozess, dann birgt sie in der Folge auch den idealen Nährboden für die Post-Privacy. Im Gegensatz zum Rückzug in den Schutz der Privatsphäre (Moderne), bietet diese nämlich zahlreiche Plattformen und Tools zum Austesten der neuen Optionen (Postmoderne). Berücksichtigt man noch weitere Nebenerscheinungen der Individualisierung, wie etwa die „Pluralisierung von Lebensstilen [...] und soziale Mobilisierung" (Krotz 2001: 241), so wird die unterstützende Form der Post-Privacy umso deutlicher. Die Konnektivität des Internet in all dessen Ausformungen multipliziert die neu gewonnenen Freiheiten um ein Vielfaches. Wo können die Optionalität der Lebensstile und Identiätsexperimente besser ausgelebt werden, als auf den Bühnen des Social Web? Andererseits hat die Post-Privacy, quasi als Speerspitze des voranschreitenden Individualisierungsprozesses, auch ein reintegratives Moment. Die befreiten Individuen werden gewissermaßen wieder in die Gesellschaft geholt. Angesichts der möglichen Überwachungsmaßnahmen, die mit der Post-Privacy einhergehen, werden sie aber sogleich einem Kontrollverhältnis unterworfen. Individualisierung bedeutet für die Einzelnen nicht nur Befreiung, sondern eben auch „Kontrolle und Reintegration durch zunehmende Abhängigkeit der einzelnen Menschen von Institutionen und Märkten." (Krotz 2001: 241) Post-Privacy kann diesen Effekt verstärken, aber auch umkehren. Wenn sich Arbeitsmärkte zunehmend flexibilisieren und pluralisieren, jede/r seinen/ihren eigenen Weg geht und einst mächtige Ge-

werkschaften ihr Fundament verlieren, dann kann Post-Privacy auch wieder solidarisieren. So kann sie eben auch als Korrektiv zum kontrollmotivierten Reintegrationsprozess der Individualisierung angesehen werden.

Das befreite und reintegrierte Individuum ist in der neuen Welt aber keinesfalls unmündig resp. ohnmächtig einer übergeordneten Macht ausgeliefert. Die Individualisierung hängt stark mit einer „vergrößerten Bedeutung individueller Reflexions- und Erwartungsprozesse" (Krotz 2001: 241) zusammen. Für das Individuum bedeutet das, dass es die neuen Möglichkeiten und Optionen durchaus reflektiert. Es fühlt sich verantwortlich für die sinnvolle und möglicherweise eigennützige Ausgestaltung der neuen Lebensbereiche. Im Kontext der Post-Privacy bedeutet dies, dass mit dem Aufkommen neuer Möglichkeiten, plötzlich auch Techniken wie Selbstdarstellung und Selbstthematisierung relevant werden. Die Umsetzung dieser Techniken setzt gleichzeitig die Bereitschaft für mehr Offenheit und Transparenz voraus. Ein Rückzug in die Privatsphäre nämlich, macht in dieser neuen Welt der Optionen unsichtbar.

So schafft Individualisierung im Konnex mit den Technologien der Post-Privacy, die Grundlage für eine Aufmerksamkeitskultur. Oder umgekehrt - um von einem Technikdeterminismus loszukommen - hat die aufkommende „Bekenntniskultur" (Burkart 2006: o.S.) den Technologien der Post-Privacy Vorschub geleistet.

2.2 Bekenntnis- und Aufmerksamkeitskultur

Als das Time Magazine 2006 ‚Dich' oder ‚Euch' mit der markanten Aussage: „Yes, you. You control the Information Age. Welcome to your world." (Gross-

man 2006: online) zur Person des Jahres kürte, wurde damit in einem Satz ein Kapitel in der Entwicklung des Internet heruntergebrochen, das als Web 2.0 oder Social Web in die Geschichtsbücher einging. Online-Services wie Youtube implizieren seither bereits in ihrer Namensgebung die verstärkte Hinwendung zum/zur NutzerIn, der/die im Zuge der aktuellen Entwicklungen, immer mehr in den Mittelpunkt rückt. Die neuen Tools bringen aber auch neue Begehrlichkeiten mit sich. Sie pluralisieren die Möglichkeiten der Selbstthematisierung und zwingen ihre UserInnen förmlich zu Bekenntnissen und Geständnissen, zur Generierung von Aufmerksamkeit. Die '15 minutes of fame' kann plötzlich jede/r erhaschen. Reichert spricht in diesem Zusammenhang von einer „Ökonomie der Aufmerksamkeit" (Reichert 2008: 60), die sich in der Ära „postindustrieller Informationsvermittlung und -verwaltung" (Reichert 2008: 60) etabliert hat.

Symptomatisch für diese Bekenntniskultur ist eine Herabsetzung der Tabuisierungsschwelle. Alles kann, alles muss angesprochen und öffentlich thematisiert werden. Was vor noch nicht all zu langer Zeit als tabu resp. unaussprechlich galt, muss der Spatz in jüngerer Zeit am Besten schon gestern von den Dächern getwittert haben. Tabu ist immer seltener das Unaussprechliche, sondern eben das Nichtaussprechen desselben: Die Bekenntnis-Verweigerung (vgl. Burkart 2006: 7). Aufmerksamkeits- und Bekenntniskultur sind aber keine Kinder der Post-Privacy. Sie werden lediglich von ihren Tools befeuert. Selbstthematisierungsprozesse gehen viel weiter zurück. Vor dem Internet, erlebten sie ihren Höhepunkt bereits im Aufkommen des Privatfernsehens in den 80er-Jahren, mit Talkshowformaten, die private Themen zunehmend in die Öffentlichkeit trugen. (Vgl. Reichert 2008: 41)

KritikerInnen warnen zwar davor, sind sich aber mit den BefürworterInnen der Post-Privacy einig und konstatieren: Die Ausweitung der Bekenntniskul-

tur ist im Zuge der Post-Privacy nicht mehr zu bremsen. Die „hoffnungslos dem Netz-Exhibitionismus Verfallenen" (Kurz/Rieger 2011: 11), die „Rampensäue" (Leggewie 2007: 48), sie alle nehmen die Tools der Post-Privacy, die Services der Social Networks mit all ihren Vor- und Nachteilen in Kauf. Ganz im Sinne der Aufmerksamkeitsökonomie.[5]

Betrachtet man diese Entwicklung aus einer ideologiekritischen Perspektive, wonach Individuen immer auch in den Kontext vorherrschender Machtverhältnisse eingebettet sind (vgl. Reichert 2008: 42), so ergibt sich aus der Ausweitung der Bekenntniskultur zudem ein enormes Potential für die Kontrolle und Steuerung der sich bekennenden Subjekte. Staatliche oder wirtschaftliche Überwachungs- und Scoring-Techniken (Kapitel 4.3) können durch die zunehmende Offenheit der Individuen stets weiterentwickelt und optimiert werden.

Post-Privacy und das Florieren der Bekenntniskultur gehen Hand in Hand. Sie bedingen resp. bewirken einander quasi gegenseitig. Die Individualisierung, als gesamtgesellschaftler Metaprozess, liegt diesen Entwicklungen als fruchtbarer Nährboden zu Grunde. Eine weitere Ebene, kommt nun mit den omnipräsenten Technologien, den Tools der Post-Privacy hinzu, welche ihren Vormarsch begünstigen.

2.3 Technologische Omnipräsenz

Neben Prozessen, wie der Individualisierung und der damit einhergehenden Ausweitung der Bekenntniskultur, ist es vor allem die technologische Durchdringung des Alltags, welche der Post-Privacy Vorschub leistet. Im sog. ‚Per-

[5] Neben der Generierung von Aufmerksamkeit und Zuspruch, stecken noch weitere Motivationen hinter der Nutzung der Transparenz-fördernden Post-Privacy-Tools. Auf diese gehe ich in Kapitel 4 ein.

vasive Computing', also der „Miniaturisierung und Einbettung von Mikroelektronik in andere Objekte sowie ihre Vernetzung und Allgegenwart im Alltag" (Bütschi/Hilty 2003: online), scheint dieser Prozess zu kulminieren. Die technologische Ubiquität spiegelt sich nicht nur in den Überwachungstechnologien im öffentlichen Raum oder dem vernetzten Computer wider. Sie geht weiter. Hin zum Körper. Von smarter Kleidung, smarten Phones bis hin zur smarten Brille.[6] Alltägliche Gegenstände werden so zunehmend mit einer Sensorik ausgestattet, „über die sie ihre Umgebung erfassen, ohne dass Benutzende dies aktiv veranlassen." (Bütschi/Hilty 2003: online) Verbunden mit der Konnektivität des Social Web, geht aus der technologischen Allgegenwart auch eine schier unfassbare Menge an Daten hervor. Genau darin sehen die Befürworter der Post-Privacy ein enormes Aggregations- und Korrelationspotenzial, welches nicht nur der Wirtschaft, sondern auch der Optimierung der Gesellschaft dienen kann. „Mining that data may become the gold rush of our age." (Jarvis 2011: 918) Wie sich dieser „Messbarkeitswahn" (Hilty 2011: Interview) auf die Individuen auswirken kann, zeige ich weiter unten (Kapitel 4.3) auf.

Bei ihren UserInnen weckt die neue Technologie jede Menge Begehrlichkeiten, die es zu ergründen gilt. Wenn die Technik schon einmal da ist, dann möchte man sie schließlich auch nutzen. Je offensichtlicher der Nutzen und je latenter die Risiken, desto eher wird sie auch angenommen. Das gilt für staatliche Überwachungsmaßnahmen genauso wie für die Einführung eines neuen Social-Media-Services. Von dieser Warte aus gesehen, ist die transparente Gesellschaft der Post-Privacy durchwegs technikdeterministisch ausgelegt. Kommt ein neues Gadget auf den Markt, dann überwiegen die Freiheiten, die es schafft. Mögliche Risiken und Einschnitte für die Privatsphäre werden im Glanz der neuen Annehmlichkeiten gerne ausgeblendet.

---

[6] Siehe hierzu etwa das Projekt Google-Glass.

In seiner Mobilität bildet heutzutage das Smartphone die Speerspitze der technologischen Omnipräsenz. Als alltäglicher Begleiter, ständig vernetzt, wird es zum ultimativen und unverzichtbaren Post-Privacy-Tool. Für das Masterprojekt Miio, haben wir ein ein solches Supersmartphone entwickelt resp. eine Fake-Version davon. Als Ideengeber war ich maßgeblich in den Konzeptionsprozess dieses Abschlusswerks involviert. Miio, eine Art Alleswisser, kann in Sekundenschnelle Personen scannen und bewerten. Dabei werden personenbezogene Daten aggregiert, kombiniert und anschließend in einen Score umgewandelt. Das Device, das stark an der Haptik eines Smartphones angelehnt ist, funktioniert dabei wie ein Fenster, durch welches UserInnen andere Personen anvisieren und scannen können und dadurch Zugriff auf praktisch alle digital erfassten Informationen und Datenschnipsel zur jeweiligen Person erhalten. Der Datenpool speist sich aus sämtlichen privaten, behördlichen, kommerziellen und öffentlichen Datenbanken: Polizeiregister, Krankenakten, Bankdaten, Daten privater Kommunikation, Daten von Payback- und Kreditkarten, sowie sämtliche Daten, die im Internet und in sozialen Netzwerken zu finden sind. Die bestehenden Gesetze zum Schutz der Privatsphäre, die ein solches Gerät heute noch verbieten würden, haben wir in unserem Szenario einmal außer Acht gelassen und mit Miio eine drastisch zu Ende gedachte und dystopische Vision von Post-Privacy geschaffen. In einem Dokumentarfilm - ich war in der Rolle des Drehbuchautors und Regisseurs - haben wir uns zudem kritisch mit den Folgen, die ein solches Post-Privacy-Tool mit sich bringt, auseinandergesetzt.

3 Forschungsstand & AkteurInnen

Post-Privacy als Begriff hat noch recht dürftige Quoten. Eine schnelle Google-Suche ergibt schlappe 600.000 Einträge. Und von denen müsste man noch jene Ergebnisse wegzählen, die ‚post' im Sinne von ‚posting', also Eintrag interpretieren. Ein mageres Ergebnis, wenn man dem die Zahl der Trefferquote von ‚Datenschutz' gegenüberstellt: knapp 400 Millionen Einträge. Von DatenschützerInnen verpönt und von der Wissenschaft ignoriert[7], fristet die Post-Privacy-Bewegung mit ihren Forderungen und Prämissen (Kapitel 3.4a) - angesichts der schieren Anzahl ihrer GegnerInnen - ein noch relativ einsames Dasein. Das Phänomen, welches sie beschreibt ist allerdings omnipräsent.

Die ausstehende Anerkennung durch die Wissenschaft, scheint der Post-Privacy-Debatte im Netz aber keinen Abbruch zu tun, denn schließlich geht es besonders ihren GegnerInnen nicht um wissenschaftliche Analysen, sondern um die Abwendung sehr dezidierter Probleme und Gefahren, die aus einer solchen Idee hervorgehen. Ihre BefürworterInnen berufen sich wiederum auf die wenigen, teils essayartigen und in die Jahre gekommenen Schriften verschiedener Transparanz-VerfechterInnen (z.B. Brin 1998). Methodisch fundiertere Ansätze zum Thema findet man in etlichen Studien, die sich mit den Symptomen einer aufkeimenden Bekenntniskultur, sowie mit den neuen Selbstpräsentationsplattformen die das Social Web hervorgebracht hat, auseinandersetzen. Wissenschaftliche Institutionen, wie etwa das Pew Internet & American Life Project, schaffen mit ihren regelmäßig veröffentlichten Studien zur Online Privacy von Jugendlichen (z.B. Pew Internet 2007: online) eine wichtige Grundlage für eine dezidiertere Beleuch-

[7] Die bestehende Post-Privacy-Debatte hat insofern ein Problem, als sie sich nicht auf bereits bestehende wissenschaftliche Arbeiten und Forschungsergebnisse beziehen kann, welche einen expliziten Konnex zum Post-Privacy-Begriff herstellen.

tung. Diese Studien erkennen durchaus den Nährboden für eine aufkeimende Transparenzgesellschaft, welchen sie auch geordnet umreißen. Sogleich liefern die Ergebnisse dieser Studien wieder Kanonenfutter für die DatenschützerInnen und deren Gegenargumente.

Nur selten wird die Ausweitung der Transparenz-Kultur optimistischer interpretiert (z.B. bei Jarvis 2011 oder Heller 2012), Gefahren und Potenziale auf die Waagschale gelegt und das Spannungsverhältnis zwischen den Risiken und den Chancen durch das Schwinden der vermeintlich klaren Grenzen zwischen Privatheit und Öffentlichkeit, beleuchtet. Ein eindeutig definierter Umriss des Themenfeldes Post-Privacy steht zum jetzigen Zeitpunkt allerdings noch aus. In diesem Kapitel werfe ich einen Blick auf einige AkteurInnen, die das Aufkeimen einer neuen Offenheit erkannt haben und dem Post-Privacy Gespenst einen Körper geben. Doch beginnen wir mit den Fakten. Was sagt uns der aktuelle Forschungsstand?

3.1 Was sagt die Forschung?

Die aktuellen Zahlen der Forschung sprechen Bände. Allein in Deutschland ist die Zahl der InternetnutzerInnen seit der Gründung von Facebook im Jahre 2004 von 35,7 Millionen auf 53,4 Millionen im Jahr 2012 angestiegen (vgl. ARD-ZDF-Onlinestudie 2013a: online). Die Anzahl derer, die Social Networks wie Facebook regelmäßig nutzen, hat sich seit Beginn der Web-2.0-Erhebungen (2007) versechsfacht (vgl. ARD-ZDF-Onlinestudie 2013b: online). Die Gruppe der potentiellen UserInnen, die ihre eigene Privatheit durch die gängige Social-Media-Praxis publik machen, hatte noch nie so viele Mitglieder wie heute und ihre Zahl nimmt rasant zu. Beste Bedingungen also für die Post-Privacy. Hinzu kommt die Erweiterung des Nutzungs-

feldes durch portable, internetfähige Endgeräte, wie Smartphones und Tablets. „Knapp die Hälfte (45 %) der 14-bis 49-Jährigen [der Deutschen, Anm. d. Verf.] geht bereits via Handy oder Smartphone ins Internet." (ARD-ZDF-Onlinestudie 2013c: online) Die mobilen Geräte werden dabei hauptsächlich zur Nutzung von Social-Network-Diensten verwendet.

Doch warum ist gerade diese Mobilität der Geräte, vor dem Hintergrund der Post-Privacy, von Bedeutung? Weil durch die Mobilität der Zugänge und die ständige Konnektivität, ein erhöhtes Datenaufkommen entsteht. Es kommt zu einer Multiplikation der Optionen, überall digitale Spuren hinterlassen zu können. Die Generierung und Erfassung der Daten wird überdies dreidimensional. Wer, was, wo gemacht hat und möglicherweise machen wird ist durch die neue Ebene der Mobilität und die Vielfalt der Verknüpfungsmöglichkeiten von Daten, immer leichter herauszufinden. Doch zurück zu den Forschungsergebnissen.

3.2 Privatsphärebekenntnisse

Die Welt - zumindest die mit neuester Technologie gesegnete, westliche und neoliberale Welt - bewegt sich auf die totale Konnektivität zu. Angesichts der Zahlen - 75% der Deutschen nutzen das Internet regelmäßig (vgl. ARD-ZDF-Onlinestudie 2013a: online) - scheint der ‚Digital Divide', die digitale Kluft zwischen den ‚On- und Offlinern', bald überwunden. Auf Grund der Tatsache, dass durch die zunehmende Vernetzung und Nutzung der Online-Medien auch immer mehr private Daten ins Netz gelangen, stellt sich die Frage, ob dieser Umstand bei der UserInnengemeinschaft überhaupt relevant ist. Anders formuliert: Sorgen sich die Menschen überhaupt um ihre Privatsphäre im Netz? Die Antwort vorweg: ja und nein. Es besteht die land-

läufige Meinung, dass gerade Jugendliche sich nicht um ihre Privatsphäre scheren würden. Diese hätten sie, durch ihre freigiebige Online-Praxis, ohnehin längst verloren. Das ist allerdings nicht ganz korrekt.

Eine Umfrage des Pew Internet & American Life Project brachte zu Tage, dass Jugendliche teilweise sehr vorsichtig bei der Veröffentlichung ihrer privaten Daten in Social Networks sind. „Many, but not all, teens are aware of the risks of putting information online in a public and durable environment. Many, but certainly not all, teens make thoughtful choices about what to share in what context." (Pew Internet & American Life 2007: online) Aus der Studie geht hervor, dass bereits mehr als die Hälfte (55%) der Jugendlichen, Profile auf diversen Social Networks pflegen. Mehr als die Hälfte dieser 55% gaben an, dass sie ihre Profile nicht für jedermann zugänglich machen würden, um ihre Online-Identitäten zu schützen. Die Zugangsbeschränkung erfolge über die Privatsphäreeinstellungen der jeweiligen Services. Die restlichen 45% gaben jedoch zu, ihre Profile ohne jegliche Einschränkungen zu öffentlich zugänglich zu machen. Die meisten (91%) bestätigten aber, dass sie die Social Networks ohnehin nur dazu nützen würden, um mit ihren FreundInnen und Bekannten in Kontakt zu bleiben. (Vgl. Pew Internet & American Life 2007: online)

Die Daten von Pew liegen sechs Jahre zurück und man könnte meinen, dass sich die explosionsartige Verbreitung von Facebook, sowie das Transparenz-Diktat von Firmengründer Mark Zuckerberg, seither auf das Online-Verhalten von Jugendlichen ausgewirkt haben. Doch auch aktuelle Studien bestätigen, dass Jugendliche sich in Datenschutz-Belangen längst nicht so naiv zeigen, wie es ihnen oft unterstellt wird. Ein Gros der UserInnen hält nach wie vor am Schutz der Privatsphäre fest und befürchtet, dass persönliche Daten, die über das Internet weitergegeben werden, von Dritten missbraucht wer-

den könnten. (Vgl. ARD-ZDF-Onlinestudie 2012c) Doch die Sorge und Furcht reicht offenbar nicht aus, um den Schutz der Privatsphäre auch einzufordern. Schließlich steigt die Zahl derer, die auf die Tools der Social-Networks zugreifen, immer weiter an, während letztere den Datenschutz immer tiefer untergraben.[8] Darin spiegelt sich das Janusgesicht der Post-Privacy wider. Die Vorteile des Neuen überwiegen die Bedenken. Einige Zweifel und Sorgen bleiben zwar bestehen, hindern aber nicht daran trotzdem mitzumachen. Das ist der Tauschhandel: Ein bisschen Privatsphäre gegen eine schier unerschöpfliche Tools zur Vernetzung und Beziehungspflege. Geht man nun von der Annahme aus, dass alles was einmal im Netz gelandet ist, sich jeglicher Kontrolle entzieht, dann kann man sich ohnehin vom alten Konzept der Privatsphäre verabschieden. Warum? Weil eben immer mehr private Informationen ihren Weg ins Netz finden, wo sie nicht mehr zu kontrollieren sind und um jegliche Schutzmöglichkeit beraubt werden. Im Netz, so das Diktum der Post-Privacy, treffen die Korrektivmaßnahmen Schutz und Kontrolle, auf Freiheit und Transparenz. Privatsphäre wird dort nicht geschützt und kontrolliert, sondern wird öffentlich und transparent.

Die Zahlen und Belege der NutzerInnen-Forschung zeigen auf, dass die Tools und Services der Post-Privacy mit offenen Armen angenommen und kaum ernsthaft hinterfragt werden. Man genießt die Vorteile der Technologie und der mit ihr einhergehenden Transparenz, welche tief in den gesellschaftlichen Alltag eindringt. Ein Mehr an Transparenz scheint zur allseits geduldeten Selbstverständlichkeit zu werden, wenngleich DatenschützerInnen nicht müde werden vor den Folgen zu warnen. Zu viel Offenheit kann schließlich an allen Ecken und Enden Begehrlichkeiten wecken: Datenmissbrauch, Identitätsdiebstahl, Scoring, Targeting etc.

---

[8] Die ‚Name-Policy' von Facebook etwa, zwingt UserInnen des Social Networks seit geraumer Zeit dazu, in den Profilen ihre realen Namen anzugeben. (Vgl. Facebook 2013: online)

Ich habe dargelegt, woher dieser populäre Transparenzdrang der Post-Privacy rührt. Welche Metaprozesse und Rahmenbedingungen dafür verantwortlich zeichnen. Im Folgenden möchte ich nun auf jene AkteurInnen eingehen, die das Post-Privacy-Phänomen schon früh erkannt haben resp. es heute vorantreiben.

3.3 Alte ProphetInnen

> Wenn ich den Ort meiner Geburt hätte wählen können, so wäre es ein Staat gewesen, in dem weder die heimlichen Schliche des Lasters noch die Bescheidenheit der Tugend dem Blick und dem Urteil der Öffentlichkeit entgehen, weil jeder den anderen kennt. (Rousseau o.J: o.S., zit. n. Perrot 1987: 631)

Schon Rousseau träumte in der Umbruchseuphorie der französischen Revolution von einer absoluten Transparenz. Vielleicht rührte seine Offenheits-Vorliebe von einer Sehnsucht in die Antike, in welcher die ‚res publica', also die öffentliche Sache noch über allem Privaten stand? Oder ist Rousseaus Traum doch als hoffnungsvoller Blick in die Zukunft, die Zeit nach der Revolution, zu deuten? Die Zeit, in welcher verbotene Heimlichtuereien sofort aufgedeckt werden können und die verdiente Anerkennung nicht im Understatement versinkt. Die Idee von Transparenz und damit die Grundidee von Post-Privacy und ihrer positiven Auswirkung auf die Gesellschaft ist nicht neu. Einen weiteren Vordenker finden wir neben Rousseau z.B. auch in Marshall McLuhan.

3.3a Marshall McLuhan - The end of secrecy

Als er in den 60er- und 70er-Jahren seine Thesen zum Ende jeglicher Geheimhaltung kund tut, beruft sich McLuhan hauptsächlich auf das Fernse-

hen als Massenmedium, welches diese Veränderungen herbeiführen würde. Vom Internet/Social Web - zumindest wie wir es seit Mitte der 90er- resp. seit Mitte der Nullerjahre kennen - kann hier noch keine Rede sein. Dennoch muten seine Ideen prophetisch an. Die folgenden Ausführungen sind Teil eines Uni-Vortrags von McLuhan im Jahr 1974.

> Another strange effect of this electric environment is the total absence of secrecy. […] No form of secrecy is possible at electric speed. […] The pattern sticks out a mile before anybody says anything about it. At electric speed everything becomes x-rayed. […] With the end of secrecy goes the end of monopolies of knowledge. There can no longer be a monopoly of knowledge in learning, education or in power. Now this – I'm not making value judges – this would seem to many people a very good thing and it may well be a very good thing. I'm simply specifying the pattern or the form that occurs when you have instant speed of electric information. You can not have a monopoly of knowledge such as most learned people had a few years ago. You can not have it under electric conditions. This applies to all professional life as well as to private life. (McLuhan 1974: online)

McLuhan glaubt, auf Grund der Geschwindigkeit, in der Information verbreitet würde und auf Grund der Beschaffenheit der Kanäle, in welcher sie verbreitet würde, sei sie nicht zu kontrollieren resp. zu verbergen. Damit weist er auf ein Problem hin, welches heute als Verlust über die informationelle Selbstbestimmung beschrieben wird. Ein Phänomen welches, wie ich aufgezeigt habe, durch die technologischen und gesellschaftlichen Rahmenbedingungen der Post-Privacy forciert wird. Sind Informationen erst einmal im Netz, lassen sie sich schwer ‚bändigen'. Dieser Umstand betrifft sodann auch alle Bereiche, welche - direkt oder indirekt - in diese elektronische Umgebung eingebettet sind. Niemand kann mehr Wissensmonopole beanspruchen. Gleichzeitig kann nichts geheim gehalten werden, d.h. mehr Wissen für alle, dafür aber auch weniger Geheimniskrämerei für alle. In diesen paar Sätzen hat McLuhan den Gedanken der Post-Privacy, Jahrzehnte bevor überhaupt die Rahmenbedingungen einer solchen geschaffen waren, auf den Punkt gebracht.

3.3b David Brin - Die transparente Gesellschaft

Etwas später kommt der Science-Fiction-Autor David Brin zum Zug. Auch er beschreibt, aus heutiger Sicht, schon sehr früh (1998) und ebenso prophetisch, wie der gesellschaftliche Transparenzschub, durch das damals noch nicht so stark verbreitete Internet vorangetrieben würde und wie wir in Zukunft lernen müssten, damit umzugehen. Bevor sich einzelne Institutionen die Überwachungs- und Steuerungsmöglichkeiten durch das Internet zu Nutze machen, müsse die Gesellschaft einen Rahmen für mehr Transparenz schaffen. Privatsphäre als gesellschaftliche Gegebenheit, sieht er vor 15 Jahren, noch vor dem Höhenflug der weltweiten Vernetzung durch das Internet, als nicht mehr länger haltbar an, wenngleich DatenschützerInnen und BürgerInnen vehement daran festhalten. Er zitiert seinen Freund John Barlow, welcher in ebenso weiser Voraussicht konstatiert:

> I have no secrets myself, and I think that everybody would be a lot happier and safer if they just let everything be known. Then, nobody could use anything against them. But this is not the social norm at the moment. (Barlow 1998: o.S., zit. n. Brin 1998: 23)

Wie wir in unserem Masterprojekt Miio, zeichnet auch Brin in seinem Beitrag zur „Transparent Society" (1998) ganz zu Beginn, ein dystopisches Szenario. Die Welt liegt zwar nicht in Scherben, dennoch sieht sie sich, neben den üblichen Umwelt- und Wirtschaftsproblemen, mit einem ganz neuen, weltumspannenden Phänomen konfrontiert: Alles was man in der Öffentlichkeit tut, wo man sich aufhält, mit wem man sich trifft etc. wird beobachtet. „The [...] change peers down from every lamppost, every rooftop and street sign. Tiny cameras panning left and right, survey traffic and pedestrians, observing everything in open view." (Brin 1998: 4) Was bereits zu Anfang einem Orwell'schen Albtraum anmutet, entpuppt sich sogleich als eigenwillige Vision. Brin prognostiziert kein zentrales Überwachungssystem. Hinter den Monito-

ren sitzen keine PolizistInnen und halten Ausschau nach DrogendealerInnen und VerkehrssünderInnen. In seiner Vorhersage können alle BürgerInnen gleichermaßen auf die Bilder der Überwachungskameras zugreifen. Menschen werden so zwar zu gläsernen PassantInnen, über deren Aufenthaltsort jede/r Bescheid wissen kann, haben aber gleichermaßen die Möglichkeit, die selbe Technologie zu nutzen um ihre MitbürgerInnen, Kinder, Ehemänner/frauen, Chefs, MitarbeiterInnen etc. auszuspähen. Brin nennt dieses Konzept „reciprocal transparency" (1998: 81), also gegenseitige Transparenz, oder umgemünzt auf informationelle Güter, welche zwischen unterschiedlichen hierarchischen Instanzen kursieren, „reciprocity of information flows." (1998: 87) In Brins Vorstellung wird so aus der totalen Überwachung - welche ohnehin nicht mehr abwendbar sei - die totale Transparenz.

Weiter unten (Kapitel 4.1) werde ich noch genauer auf das Prinzp der reziproken Transparenz eingehen. Ungeachtet der resignierten Grundhaltung dieser Argumentation - wenn schon Überwachung, dann für alle! - haftet ihr dennoch etwas verlockendes an, zumindest auf den ersten Blick. Bevor wir in einen 1984-anmutenden einseitigen Totalüberwachungsstaat abdriften, wäre es vielleicht besser wir drehen den Spieß um und weiten die Transparenz auf alle hierarchischen Ebenen einer Gesellschaft aus, mit wechselseitiger Offenheit aller Informationsflüsse. Kurz: Das Prinzip ‚Jede/r weiß alles über jede/n' ist besser als ‚Wenige wissen alles über jede/n.'

3.4 Neue VerfechterInnen

Mehr Transparenz, insbesondere in Informationsflüssen, fordern auch zeitgenössischere AkteurInnen in der Post-Privacy-Debatte. Sie vereint IMHO zu allererst der Wille und Drang zur Bewusstseinsschaffung. Da wäre zum Ei-

nen, die ‚Datenschutzkritische Spackeria', welche es auf den Datenschutz in Deutschland und Europa abgesehen hat und die Debatte auf politischer Ebene neu aufgerollt wissen will (vgl. Fasel 2011: online). Ihre Forderungen werden weiter unten (Kapitel 3.4a) noch genauer beleuchtet. Ebenso zur Post-Privacy-Runde gesellt sich ein bekennendes und regelmäßig kontribuierendes Mitglied der ‚Datenschutzkritischen Spackeria', welches ich speziell hervorhebe, namentlich Christian Heller alias Plomlompom. Er hat durch seinen Post-Privacy-Vortrag auf dem Chaos Communication Congress 2008 (vgl. Chaos Communication Congress 2008: online) für Furore unter DatenschützerInnen gesorgt. Mit seiner jüngsten Bucherscheinung (2011) hat er den bisher umfangreichsten, monographischen Beitrag zum Thema geleistet und ist damit ebenso ein maßgebender Akteur im Dickicht der Post-Privacy-Debatte. Auch er erhebt sich gegen einen zu streng gelebten Datenschutz. Ein weiterer Protagonist in der Post-Privacy-Debatte findet sich auf der anderen Seite des großen Teichs. Jeff Jarvis, ein US-amerikanischer Journalistik-Professor[9], genießt ebenso eine Sonderstellung, da er relativ radikale Forderungen nach mehr Transparenz stellt und dabei sehr öffentlichkeitswirksam agiert. In seinem Buchbeitrag „Public Parts. How Sharing in the Digital Age Improves the Way We Work and Live" (2011) fordert er, dass man sich in der neuen durchtechnologisierten „Age of Publicness" (Jarvis 2011: 82) nicht nur auf die Risiken für die Privatsphäre, sondern auch auf die Vorteile von Öffentlichkeit und Transparenz konzentrieren sollte. „Privacy has its advocates. So must publicness." (Jarvis 2011: 138) Weitere wichtige Schlüsselfiguren im Post-Privacy-Dunstkreis sind natürlich die Konzerne, die Social-Networks und Suchdienstanbieter, Google, Facebook, Amazon und die Hardwarehersteller, welche die neue Transparenz nicht nur propagieren, sondern von der mit ihr einhergehenden Datenflut auch profitieren.

[9] Der New York Observer verlieh im das Prädikat „Web Guru." (Koblin 2008: online)

3.4a Post-Privacy-Spackos

Der ‚27C3', also der 27. Chaos Communication Congress in Berlin war es, der im Frühjahr 2011 genügend Anlass zur Gründung der ‚Datenschutzkritischen Spackeria' gab. Das Fass zum Überlaufen brachte Constanze Kurz, Pressesprecherin des Chaos Computer Clubs, die jene Datenschutz-kritische Riege mehrfach als „Post-Privacy-Spackos" (Kurz 2011: o.S., zit. n. Seeliger 2011: online) beschimpfte und sogleich auch als Namensgeberin der Bewegung einstand.

Auf ihrer Plattform blog.spackeria.org wird seither lebendig zu den Themenfeldern rund um die Post-Privacy diskutiert und disputiert. Zu Beginn, aber auch heute noch wurden und werden die Vorschläge der Community missverstanden. Häufig werden ihre Forderungen als utopisch und weltfremd erachtet. Besonders aus dem Lager der DatenschützerInnen fühlt man sich durch die Forderungen Datenschutz-SkeptikerInnen nach mehr Transparenz, untergraben. So erteilt man ihnen von Seiten des Chaos Communication Congress Podiums, welches sich für eine Forcierung eines EU-weiten Datenschutzes einsetzt, sogleich auch eine Absage. „Wir haben ja nichts dagegen, dass sich Leute im Netz nackig machen können. Man soll es nur nicht als Lebensstil, als soziale Norm propagieren." (Kurz 2011, zit. n. Seeliger 2011: online) Frank Rieger, der zusammen mit Constanze Kurz ein Post-Privacy-kritisches Buch geschrieben hat, geht ebenfalls in die Kritik: „Wir halten Post Privacy als Lebensstil für einen Irrweg." (Rieger 2011, zit. n. Seeliger 2011: online) Bei genauerem Durchsehen der Forderungen der Spackeria, wird allerdings deutlich, dass es ihren Mitgliedern eher um einen Diskussionsanstoß, denn um die Propagierung eines rein offenen und transparenten Lebensstils geht.

Was wollen wir?
- Problembewusstsein schaffen.
- Begriffe klar definieren, insbesondere den Begriff Datenschutz, mit dem innerhalb einer Netzbewegung oft unreflektiert umgegangen wird.
- Breiten, ergebnisoffenen Dialog zu den grundlegenden Fragen und Problemen rund um den Datenschutz.
- Ängste nehmen.
- Technik erklären.
- Gruselgeschichten abschwächen (Stichwort: Saufbilder & Co).
- Fernziel: Ausweg aus traditionellem Datenschutz vs. Transparenz-Denken.

Was wollen wir nicht?
- Den Menschen Angst machen oder ihre Privatsphäre wegnehmen.
- Datenschutzregeln aufheben um Geschäftsmodelle anzufeuern (Google/Facebook).
- Die starken Grundlagen von Datenschutz gegen den Staat in Deutschland aus Volkszählungsurteil usw. zurücknehmen. (Fasel 2011: online)

Aus diesem Leitbild spricht mehr das Aufbegehren (das Namenspräfix ‚datenschutzkritisch' suggeriert es ja bereits) gegen die Allmacht und Ohnmacht des Datenschutzes, welcher in Deutschland einen relativ großen Wirkungsbereich hat und gleichzeitig die Belange der Privatsphäre-Debatte für sich beansprucht. So geht es den Mitgliedern der ‚Datenschutzkritischen Spackeria' wohl eher darum, den DatenschützerInnen ein wenig Wind aus den Segeln zu nehmen, die allgemeine Überwachungspanik zu reduzieren und gleichzeitig auf die Gefahren und Freiheitsbeschränkungen hinzuweisen, die ein zu vehement forcierter Datenschutz bewirken kann.

3.4b Plomlompom gegen den Datenschutz

Ein Mitbegründer und Rädelsführer der ‚Datenschutzkritischen Spackeria' ist Christian Heller, im Netz unter dem Pseudonym ‚Plomlompom' unterwegs. In seinem Buchbeitrag (2011) geht er mit den AgentInnen des Datenschutzes hart in die Kritik. Den Kampf zur Rettung der Privatsphäre hält er für längst verloren. Er sieht zwar ein, dass die Privatsphäre mehr denn je von

allen Seiten bedrängt wird, erkennt deshalb aber „nicht den Auftrag, die Privatsphäre entschlossen zu verteidigen." (Heller 2011: 81) Auch er widmet sich den Chancen, die das Wegkommen von einer zu scharf verteidigten Privatsphäre und das Hinkommen zu mehr Transparenz, bietet. „Was es uns an Freiheit bringt, nicht beobachtet zu werden, das wird in mancher Weise überschätzt. Hingegen eröffnet uns der Pfad, der uns in die Post-Privacy führt, viele neue Freiheitsräume." (Heller 2011: 81) Was Brin schon Jahrzehnte zuvor postuliert, das Ende der Privatsphäre, hat sich nach Heller bereits längst vollzogen. Sein Überblick zur Situation der Privatsphäre verheißt zunächst nichts Gutes.

> Die Zahl der Augen und Ohren um uns herum steigt. Ebenso steigt die Zahl der freiwilligen oder unfreiwilligen, böswilligen oder einfach nur fahrlässigen Informanten. Das Verbreiten von Daten fällt immer leichter. Die Menge an Daten über unsere Welt explodiert und ist immer mehr Interessierten zugänglich. Ebenso schnell wächst die Intelligenz, sämtliche Puzzleteile zusammenzufügen, um aufzudecken, was noch geheimgehalten wird. All das staut sich auf zu einem gewaltigen Druck gegen die Privatsphäre als Raum des Verborgenen. Die Orte, Gelegenheiten und Sachverhalte, die sich vor diesem Druck sicher glauben können, schrumpfen in Zahl und Größe. Es fällt immer schwerer, sie zu verteidigen. (Heller 2011: 351)

Somit schreibt Heller allen AkteurInnen in diesem Post-Privacy-Umfeld eine gewisse Ohnmacht zu. Die MitmacherInnen aber auch die GesetzgeberInnen und ganz besonders die DatenschützerInnen müssten vor dem Unausweichlichen kapitulieren. „Wir können natürlich weiter Gesetze erlassen, die diese Wirklichkeit kriminalisieren. Das heißt aber nicht, dass diese Gesetze das Gewünschte bewirken." (Heller 2011: 321) Der Datenschutz, der in Deutschland eigentlich durch eine starke Lobby vertreten ist, nimmt eine zunehmend passive Rolle ein. „Datenschutz hält sich zurück oder wird zurückgehalten. Es mangelt ihm an politischer Durchsetzungskraft, an Reichweite und an Mitteln." (Heller 2011: 1482) Er wird zum Opfer der pervasiven und ubiquitären Technologie. Noch nicht 'post' genug für die Post-Privacy,

hinkt er ihren Gegebenheiten hinterher und leidet angesichts eines rasanten technologischen Wandels unter einem enormen Vollzugsdefizit. Heller glaubt, dass genau diese Ohnmacht den Datenschutz erträglicher macht. „Würde der deutsche Datenschutz vollends verwirklicht, das Internet wäre nicht wiederzuerkennen." (Heller 2011: 1482) So wichtig er in manchen Fällen auch sein mag, so kann er in konsequenter Durchsetzung, auch viele Freiheiten nehmen. Heller gefällt die Vorstellung des Datenschutz als „Brückentechnologie." (Seemann 2011: online) Demnach biete uns der Datenschutz, der ohnehin gegen Windmühlen kämpft, lediglich eine Verschnaufpause, etwas mehr Zeit im Übergang in die neue transparente Gesellschaft.

> Er [der Datenschutz, Anm. d. Verf.] besitzt keinen Freibrief, sich die Datenwelt ganz und gar zu unterwerfen, aber die Erlaubnis, die Datenwelt beim Eintreten in unser Leben um Vorsicht zu bitten. [...] Er steht vor der Wahl seine Kontrollansprüche zurückzuschrauben - wie Eltern, die ihre Kinder langsam in die Selbständigkeit entlassen - oder aber umso aggressiver für seine Kontrollansprüche zu kämpfen. (Heller 2011: 1491)

Neben seiner Kritik gegenüber dem Datenschutz hegt Heller auch Zweifel an einem zu einseitigen Verständnis von Transparenz. Mit der Hackerethik des Chaos Computer Club - „Öffentliche Daten nützen, private Daten schützen." (Chaos Computer Club 2013: online) - kommt er nicht wirklich zurecht. Dieses Modell ignoriere nämlich den oben beschriebenen Umstand, dass dieser Schutz der privaten Daten, diese Privatsphäre für die Kleinen gar nicht mehr möglich sei. Es wird also etwas suggeriert, was selbst gar nicht mehr existiert resp. haltbar ist und schafft somit falsche Behaglichkeit. Transparenz von oben mag gut und recht sein. Der Glaube, dass umgekehrt die eigenen, privaten Daten im Verborgenen bleiben, sei jedoch Augenauswischerei. Er beruft sich sodann auf Brins Konzept der gegenseitigen Transparenz (vgl. Brin 1998: 80ff). Wenn die gemeinen BürgerInnen schon keine Privatsphäre mehr genießen können, dann soll dies zumindest auch für die Regierungen,

Exekutive, Konzerne etc. gelten. Umgemünzt auf ein Überwachungsszenario hieße das, dass man die Überwachungstools allen zur Verfügung stellen soll, nicht nur den Mächtigen. Wenn Regierungen Überwachungskameras, Drohnen und Abhörstationen einsetzen um ihre BürgerInnen zu kontrollieren, dann sollte genau das umgekehrt auch möglich sein. Wenn Unternehmen ihre MitarbeiterInnen und KundInnen durch überbordende Datenaggregationen ausforschen, dann sollte auch das auf Gegenseitigkeit beruhen. Zumindest aber sollten die Prozesse und Absichten der Datenverarbeitung offengelegt werden. „Wenn wir schon nackt sein sollen, dann sollen alle füreinander nackt sein, egal ob oben oder unten, klein oder groß, gut oder schlecht. Statt die Beleuchtung durch die Überwachung nur in eine Richtung zu lenken, soll sie den gesamten Raum ausfüllen, soll jeder alles sehen können." (Heller 2011: 1781) In dieser nahezu utopisch anmutenden transparenten Gesellschaft, so Heller, könne man dann, abgesehen von der Gleichberechtigung in Überwachungsfragen, noch etliche weitere Vorteile genießen. Zum Einen sorgt Transparenz für mehr Solidarität, da man Gleichgesinnte schneller finden und im Bedarfsfall auch konsolidieren kann (vgl. Heller 2011: 2156). Ob aus dem solidarischen Bündel dann ein Flashmob oder eine Revolution entspringt sei dahingestellt. Die Tools der Transparenz sollen es jedenfalls möglich resp. einfacher möglich machen. Weiters sorgt mehr Transparenz auch für Optimierungsprozesse in der Gesellschaft. Um dies zu verdeutlichen zieht Heller die Dynamik der Wissenschaft als Beispiel heran. „Die Wissenschaft lebt von der Transparenz ihrer Theorien. Dass Theorien für jedermann einsehbar, überprüfbar und kritisierbar sind, führt zu ihrer fortwährenden Verbesserung." (Heller 2011: 2205) Eine ausführliche Beleuchtung dieser Chancen und Risiken erfolgt weiter unten in Kapitel 4.

3.4c Jeff Jarvis der Transparenz-Guru

Mit im Boot der TransparenzverfechterInnen sitzt der US-amerikanische Blogger und Journalistik-Professor Jeff Jarvis. In seinem Buch „Public Parts. How Sharing in the Digital Age Improves the Way We Work and Live" (2011) singt er ein Loblied auf die neue Transparenz, die nach seinem Erachten, technologisch bedingt ist. Bereits der Untertitel suggeriert, dass nicht ‚wir' es sind die unsere Art zu leben und zu arbeiten bestimmen, sondern die Kultur des Teilens und die Technologien im digitalen Zeitalter. Damit nimmt Jarvis eine technikdeterministische Grundhaltung ein. Die Technik verändert uns, nicht wir die Technik. Ein Journalist und Datenschützer, der sein Buch ebenfalls gelesen hat, rezensiert etwas drastischer und schreibt Jarvis eine „Geringschätzung gegenüber dem Einzelnen und seiner Freiheit, eigene, unabhängige Entscheidungen zu treffen" (Lischka 2011: online) zu.

Jarvis sieht die Grenzen zwischen Privatheit und Öffentlichkeit zunehmend im Schwinden. „We bring our private identities to our public acts - we decide in private where we stand on an issue, and making that public is what allows us to join with like thinkers, share our ideas, and organize action." (Jarvis 2011: 142) Das heißt nicht, dass aus Privatsphäre nun automatisch Öffentlichkeit wird resp. sich die Privatsphäre ganz auflöst. Wir entscheiden immer noch selbst was privat bleibt und was an die Öffentlichkeit soll oder darf. Jarvis wird zwar nicht müde, dies immer wieder zu betonen, ob er wirklich daran glaubt, sei allerdings dahingestellt. Ein Festhalten an zuviel Privatheit in diesem Zeitalter, hält er jedenfalls für wenig sinnvoll. „If we become too obsessed with privacy, we could lose opportunities to make connections in this age of links." (Jarvis 2011: 153) Im Gegenzug zu Heller schreibt Jarvis dem Datenschutz aber nicht etwa Ohnmacht, sondern vielmehr eine Übermacht zu, deren allgemeine Panikmache man sich nicht zu sehr zu Herzen

nehmen sollte. „These privacy advocates swarm in the media every time a new online service entices us to share something about ourselves. They say we should fear the companies and technologies that use the bait of free content and services, improved social lives, personalization, and increased relevance to get us to open up." (Jarvis 2011: 117) So echauffiert er sich z.B. an der deutschen Google-Streetview-Diskussion, im Zuge derer das sog. ‚Verpixelungsrecht' eingeführt wurde. Danach wurde allen bundesdeutschen BürgerInnen das Recht eingeräumt, ihre Häuser, Wohnungen und Büros, auf Google Streetview verpixeln, also unkenntlich machen zu lassen. Das Problem hier ist, dass das Verpixelungsrecht, möglicherweise die Rechte resp. Freiheiten anderer Personen, die dieses Recht nicht einfordern, einschränken kann. Der Schluss: Wenn Google keine Straßenzüge fotografieren darf, dürfen Hobbyfotografen, Journalisten etc. dann plötzlich auch nicht mehr im öffentlichen Raum fotografieren (vgl. Jarvis 2011: 517)? Damit stellt er die Street-View-Verpixelung auf eine Ebene mit öffentlicher Zensur.

Die Vorteile von mehr Transparenz und Öffentlichkeit liegen für ihn auf der Hand. Die Vorstellung, dass durch die Link-Struktur des Internet, jede/r eben nur einen Link voneinander entfernt sei, bringe ganz neue Chancen für Beziehungen hervor. Öffentlichkeit bringe die Menschen zusammen. Nur wer sich zu erkennen gibt und einbringt, wird auch erhört resp. gefunden. Vom Austausch auf diversen Social Networks, der pragmatischen Lösung eines Problems via ask.com bis hin zur Mitarbeitereinstellung via LinkedIn oder der Partnerwahl auf Elitepartner.de, „to make those connections, we must be public and share." (Jarvis 2011: 805) Offenheit bringt nach Jarvis' Meinung allen was, eben auch den Konzernen. Es müssen auch nicht zwangsläufig böse Absichten dahinter stecken. Wenn eine Softwarefirma, im Sinne der Transparenz, ein Produkt als beta-Version veröffentlicht, unvollständig und unausgereift, dann ist dies ein Hilferuf nach Kollaboration. Vielleicht gibt es

ja eine Gruppe findiger Programmierer, die das Problem lösen. Der Verdacht liegt zwar nahe, dass Firmen unter dem Deckmantel des Social Web, Crowdsourcing betreiben, um selbst Kosten einzusparen. Jarvis sieht die Sache allerdings entspannt pragmatisch: Man nutzt die Menschen nicht aus, sondern gibt ihnen die Möglichkeit, Produkte mitzugestalten. Das kann als Zeichen der Wertschöpfung gedeutet werden, was wiederum beziehungsfördernd ist. „Opening up in such a way gives customers a mesure of respect. […] The goal is to move the customer up the chain […] hearing from customers earlier to act on what they say." (Jarvis 2011: 846-856)

Jarvis nennt noch weitere Vorteile. Wenn ganze Bibliotheken digitalisiert und den Menschen über das Netz zugänglich gemacht werden, dann baut dies Schranken ab. Wissen wird für jedermann zugänglich gemacht. Die Formel lautet: „The more we open, gather, analyze, and share our knowledge, the more we all know." (Jarvis 2011: 873) Google Books und Wikipedia sind zwei populäre Beispiele dafür, genauso wie bereits das Internet an sich. Das Netz als Text- und Bildersammlung mit ihrem Hypertext, bildet bereits eine Art Alexandrinische Bibliothek der Neuzeit, die über Suchmaschinen zugänglich gemacht wird. Google Search entwickelt seine Suchalgorithmen ständig weiter und liefert in Bruchteilen einer Sekunde, Millionen Ergebnisse, akribisch nach Relevanz sortiert.

Jarvis hebt weiters, am Beispiel des arabischen Frühlings, die Tools und Optionen zur Konsolidierung einer kritischen Masse hervor. Twitter, Facebook und Konsorten können die Menschen bei der Organisation einer Revolution unterstützen. Dienen sie in Zeiten der Repression, sofern sie nicht von den Unterdrückern verboten werden, noch als Tools für den Guerilla-Aufstand, so können sie nach dem Sturm auch dazu genutzt werden ein neues System zu etablieren. Zusammengefasst: „Publicness organizes us." (Jarvis 2011: 1023)

3.4d Die Profiteure

Wichtige AkteurInnen in der Post-Privacy-Diskussion sind natürlich auch jene Konzerne und Firmen, die von verstärkter Datenfreigabe profitieren. Facebook, Google, Amazon - um nur die ‚Big 3' zu nennen - leben von den Daten ihrer UserInnen. Angesichts des Umstands, dass die meisten Social Media Dienste ihre Services kostenlos anbieten, werden die fehlenden Einnahmen häufig durch eine Monetarisierung der NutzerInnendaten kompensiert. Das passiert zu einem Großteil über den Verkauf der Daten und deren Verwertung für Werbezwecke. Je mehr Daten angesammelt werden, je akribischer die KundInnenprofile ausgestaltet werden, desto mehr Profit lässt sich daraus schlagen. Da ist es nicht verwunderlich, dass Google und Konsorten, in der Gesellschaft zu mehr Offenheit aufrufen. DatenschützerInnen sehen darin die Ironie der gesamten Post-Privacy-Debatte, welche eigentlich nur den wirtschaftlichen Nutznießern in die Hände spiele. „Nicht zufällig sind die Profiteure der Netzökonomie dieselben, die nicht müde werden zu betonen, dass die analogen Zeiten vorbei seien, in denen wir noch selbst bestimmen durften, was wir von uns preisgeben - Privacy is dead, you know." (Kurz/Rieger 2011: 88)

Doch genau an dieser Schnittstelle werden immer wieder Kosten und Nutzen der Post-Privacy ausgehandelt. DatenschützerInnen werden zwar nicht müde, auf die Gefahren hinzuweisen, die mit dem lockeren Umgang privater Daten einhergehen, die NutzerInnen scheinen davon aber unbeeindruckt zu bleiben. Für sie sind die Chancen oft greifbarer als die Risiken, die verborgen irgendwo im Hintergrund schlummern und nur ein Einzelfällen, etwa bei Identitätsdiebstahl oder Cybermobbing, zum Verhängnis werden. Der Tauschhandel ‚Daten gegen Sociality', scheint zum unhinterfragten Standard ge-

worden zu sein, zur klassischen ‚Win-Win-Situation'. Nimmt uns die Post-Privacy tatsächlich unsere Selbstbestimmung und Kritikfähigkeit? Macht ihr Glanz uns blind für Risiken, die sie mit sich bringt? Oder sollten wir die Sache entspannter sehen, kapitulieren, die Win-Win-Situation akzeptieren und einen pragmatischeren Blick auf die Chancen der Post-Privacy werfen, anstatt sie prinzipiell abzulehnen?

Durch das Aufzeigen einiger Chancen und Risiken der Post-Privacy, die sich fallweise auch als Trugschlüsse entpuppen können, gehe ich diesen Fragen im nächsten Kapitel auf den Grund.

4 Chancen, Risiken, Trugschlüsse

Naturgemäß ergeben sich aus der Vorstellung einer völlig transparenten Welt, in der der/die gemeine BürgerIn zum kalkulierbaren Datensatz wird, jede Menge Risiken. Der radikale Wandel unserer Gesellschaft, bedingt durch oder verbunden mit einem rasanten technologischen Wandel und einer zunehmenden Verlagerung privater Lebensbereiche in die Öffentlichkeit, kann jedoch durchaus gesellschaftliche Vorteile bieten.

Die Risiken sind offenkundig. Sie reichen von den häufig beschriebenen Überwachungs- und Scoring-Dystopien in Orwell-, Huxley oder Samjatin-Manier, bis hin zu ganz konkreten Beispielen, wie etwa Datenklau und Identitätsdiebstahl oder Cyberbullying. Vor dem Hintergrund dieser dezidierten Fälle müssen wir uns auch die Frage stellen, inwieweit die ausufernde Datentransparenz auch einen Angriff auf die Menschenwürde darstellt. Oder wie durch fehlerhaft interpretierte Datensätze all zu leicht Fehlschlüsse über eine Person gezogen werden.

DatenschützerInnen glauben, dass hinter der Stimmungsmache für die Post-Privacy und dem Ende der Privatsphäre, rein monetäre oder Kontrollmotivierten Interessen von staatlichen und wirtschaftlichen Institutionen stecken. Demokratische Grundrechte würden dadurch schleichend ausgehebelt. Post-PrivatistInnen halten entspannt-pragmatisch dagegen. Im folgenden Kapitel wird dieses nicht abklingende ‚Für-und-Wider' genauer besehen.

4.1 Gleichheit durch Transparenz - Chance oder Trugschluss?

An dieser Stelle möchte ich noch einmal auf die Argumentationsstränge von Post-Privacy-Vordenker David Brin eingehen. Selbiger sah in der Ausweitung der Informationsflüsse in alle Richtungen, durch alle Hierarchiestufen durch, die bessere Alternative als den ohnehin unausweichlichen Überwachungsstaat, wie er mit prophetischem Pathos ausführt: „We may not be able to eliminate the intrusive glare shining on citizens of the next century, but the glare just might be rendered harmless through the application of more light aimed in the other direction." (Brin 1998: 23) Wenn schon Überwachung, dann für jede/n! Dieser Argumentation liegt ein einfaches Prinzip zu Grunde. Wissen ist Macht. Wissen wird durch Transparenz zugänglich gemacht. Je transparenter die Gesellschaft, desto offener ist dieser Zugang zu Wissen, desto mächtiger sind die, die sich dieses Wissen aneignen und zu Nutze machen. Haben also beispielsweise nur staatliche Institutionen oder mächtige Großkonzerne Zugang zu den akribisch geführten Datenbanken über BürgerInnen, KundInnen, möglichen VerbrecherInnen etc., so sprechen wir von Machtkonzentration und drohen mit diesem Szenario in dystopische Verhältnisse à la Orwell und Huxley abzudriften. Dabei werden BürgerInnen zu entmachteten und entdemokratisierten Spielbällen der großen Wissenshüter. Doch was passiert, wenn man den Spieß umdreht und den BürgerInnen die Waffen der Obrigkeit in die Hand drückt? Wenn plötzlich jede/r gleichermaßen das Recht hat im Regierungsapparat rumzuschnüffeln, Polizeiakten zu begutachten oder das Finanzgebaren der Bank, des Arbeitgebers, der Regierung zu durchforsten. Dann sprechen wir von Brins transparenter Gesellschaft, in welcher nicht nur der Blick von oben nach unten möglich ist, sondern auch der von unten nach oben und zur Seite. Macht- und Autoritätshierarchien sollen durch reziproke Informationsflüsse also abgebaut werden.

DatenschützerInnen sehen in dieser „leicht naiven Vorstellung" (Kurz 2011: Interview) vom Abbau der Machhierarchien durch mehr Transparenz, wenig Logik. An einfachen Beispielen, etwa an der Gegenüberstellung ChefIn-Angestellte/r, SchülerIn-LehrerIn, Eltern-Kinder, Grenzbeamte/r-Reisende/r etc. ließen sich autoritäre Ungleichheiten trotz oder gerade wegen gegenseitiger Transparenz festmachen. (Vgl. Kurz 2011: Interview).

Dieser Argumentationskette liegt außerdem ein weiteres Problem zu Grunde. Reziproke Transparenz mag zwar in all ihrer Konsequenz gewisse Vorteile für eine Gesellschaft hervorbringen und gar gerecht erscheinen. Die einzelnen Akteure in diesem Informationsgeplänkel, seien es private Personen, global agierende Unternehmen oder staatliche Institutionen, werden auf der anderen Seite aber immer versucht sein, im Sinne ihrer eigenen Interessen zu agieren. D.h. Ich als private Person werde zwar versuchen möglichst viel über mein Versicherungsinstitut, dessen Finanzgebaren und Vertrauenswürdigkeit in Erfahrung zu bringen, fühle mich gleichzeitig aber in meiner Privatsphäre gestört, wenn das selbe Institut, intimste Parameter meiner Persönlichkeit heranzieht und mich darauf basierend ob meiner Versicherbarkeit prüft. Umgekehrt werden dem Institut meine Schnüffeleien im Firmentresor ebenso missfallen. Diese Dynamiken hat bereits Brin als Problem erkannt. „Whenever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everybody else." (Brin 1998: 12) Uneingeschränkte Transparenz fordert man immer nur von den anderen, den Bösen, während man selbst, als Gute/r, die Hoheit über die eigene Privatsphäre wahren möchte.

Auf Grund dieses Dilemmas wird eine völlig transparente Gesellschaft auch kaum realisierbar sein. Persönliche Interessen, betreffend die Privatsphäre, haben darin nämlich nichts verloren. Brin gibt auch zu, dass die Vorstellung

einer Transparenten Gesellschaft sehr stark auf der Verantwortung der in ihr lebenden und agierenden Individuen fußt. Die funktionierende transparente Gesellschaft setzt voraus, dass niemand den Informationsfluss missbraucht und dass alle Informationsflüsse uneingeschränkt reziprok verlaufen. Ein Ungleichgewicht in den Informationsflüssen führt unmittelbar zu Machtassymetrien. Zur Verdeutlichung von Brins Verantwortungsmodell (vgl. 1998: 86) in der Transparenten Gesellschaft könnte man einen simplen Spruch heranziehen: Was du nicht willst das man dir tut, das füg auch keinem anderen zu. Und sollten Informationen dennoch einmal missbräuchlich verwendet werden, dann unterstützen die Offenheit des Systems und die Tools der gegenseitigen Überwachung bei der Ausforschung der ÜbeltäterInnen.

4.2 Überwachung vs. Transparenz

Gerade im Bezug auf das Thema Überwachung fährt man in der Post-Privacy-Diskussion zweigleisig. Überwachung ist zunächst einmal negativ konnotiert. Wenn z.B. Instanz A, Instanz B, möglicherweise ohne deren Wissen, überwacht, dann entsteht Asynchronität im Machtgefüge, wie ich weiter oben schon geschildert habe. Eine Instanz weiß mehr über die andere und nutzt dieses Wissen zu ihrem Zweck. Das ist ungerecht, aber offensichtlich Teil unseres täglichen Lebens. Wie aber sieht es aus, wenn man diese Hierarchie abschafft? Wenn Instanz A und B die selben Möglichkeiten der gegenseitigen Überwachung haben? Wird Überwachung somit plötzlich gut oder zumindest gerecht? Bevor ich auf diese Grundüberlegung der Post-Privacy-Theorie genauer eingehe und damit die Bedenken zu einem Big-Brother-ähnlichen Überwachungsstaat z.T. neutralisiere, möchte ich über einen anderen Zugang zum Thema Überwachung und Post-Privacy einführen und die Ausgangslage beschreiben.

4.2a Überwachung ist überall

Sieht man von den seit Beginn der 90er-Jahre in Großbritannien und auch dem Rest der westlichen Welt massiv forcierten Überwachungsmaßnahmen (ausführlich beschrieben von Kammerer 2008: 74f), meist in Form von CCTV (Überwachungskameras im öffentlichen Raum), ab, so ist Überwachung auch in vielen anderen Lebensbereichen nahezu ubiquitär. Meist findet diese Überwachung nach einem Top-Down-Prinzip statt. So überwacht etwa ein Staat oder ein global fungierender Konzern, eine breite Masse, oft ohne deren Wissen resp. bewusster Wahrnehmung. Legitimiert werden die Maßnahmen - wenn sie etwa vom Staat lanciert werden - hauptsächlich als solche zur Bekämpfung von Kriminalität und Terrorismus. Doch haben sie sich erst einmal etabliert, wachsen damit die Begehrlichkeiten, die Überwachung auch auf andere Lebensbereiche auszuweiten, ohne dabei großes Aufsehen zu erregen.[10] „Überwachung ist durch und durch alltäglich" (Kammerer 2008: 85) und „weder exzeptionell noch konspirativ, sondern wie selbstverständlich eingeflochten in das Gewebe des sozialen und privaten Lebens, Kommunizierens, Verhandelns." (Kammerer 2008: 85)

Diese Omnipräsenz und Alltäglichkeit manifestiert sich, wie erwähnt, bei weitem nicht nur im klassischen CCTV. Man denke an die Smartphones, die eine/n täglich begleiten und fallweise gar die zurückgelegten Wege mitspeichern (vgl. Neumann 2011: online). Nicht zu vergessen, die Spuren, die wir im Netz auf jeder besuchten Seite hinterlassen, auf Facebook, oder mit den im Hintergrund geschehenden Check-In's auf Foursquare. Unsere Kreditkartenkäufe, der Gebrauch der Rabattkarte im Supermarkt oder der E-Card im Krankenhaus - um nur die Spitze des Eisbergs zu nennen - alles wird ir-

[10] Die Technikforschung kennt dafür den Begriff der schleichenden Ausweitung der Funktionen (function creep) eines Systems. (Vgl. Kammerer 2008: 92)

gendwo, irgendwie protokolliert, aggregiert und ausgewertet.[11] „Solche Mikro-Überwachungen operieren (normalerweise) nicht im Konspirativen, sondern schlicht unterhalb der Wahrnehmungsschwelle, weshalb sie die meiste Zeit unserer Aufmerksamkeit entgehen. (Kammerer 2008: 85)

Dieses Prinzip der fortwährenden und insbesondere auf die Erhebung von Daten beruhenden Überwachung, nennt Roger Clarke „dataveillance" (1988: 499) sprich, „the systemic use of personal data systems in the investigation or monitoring of one or more persons." (ebd. 1988: 499) Denkt man diese Aussage konsequent durch, dann ist der Euphemismus Informationsgesellschaft längst zum Schreckgespenst, der Überwachungsgesellschaft mutiert. „All societies that are dependent on communication and information technologies for administrative and control processes are surveillance societies." (Lyon 2001: 1) Markus Beckedahl, der Betreiber des Blogs netzpolitik.org bringt sein Empfinden dazu trocken auf den Punkt. „Es ist nicht mehr die Frage ob der Staat uns überwacht, sondern wer überwacht uns noch. [...] Wir leben zwar noch nicht in einem totalitären System wie Orwell es geschaffen hat aber wir leben ganz deutlich in einer Überwachungsgesellschaft." (Beckedahl 2011: Interview) Auch er verweist dabei auf die oben geschilderten Datenspuren, die BürgerInnen wissentlich oder unwissentlich aber doch täglich generieren.

4.2b Überwachung bietet Vorteile

Dataveillance passiert jeden Tag. In einer Gesellschaft, die ein ausgeprägtes Bewusstsein zum Schutz der eigenen Privatsphäre und zum Schutz vor Überwachungsmaßnahmen ausgebildet hat, ist diese Form der Überwa-

[11] Auf das Scoring, die Folge der Summe all dieser Mikro-Überwachungsmaßnahmen durch Datenaggregierung, gehe ich weiter unten (Kapitel 4.4) noch genauer ein.

chung allerdings schwieriger zu legitimieren. Und genau hierin liegt die Krux resp. hier kommt der Begriff Post-Privacy ins Spiel. All jene Überwachungsmaßnahmen, seien sie staatlicher oder kommerzieller Natur, müssen nicht gewaltsam gegen den Widerstand der BürgerInnen durchgesetzt werden, insbesondere die weiter oben beschriebenen, latenten Maßnahmen. „Überwachung ist nicht der Gesellschaft aufgezwungen, sondern integrale, notwendige Voraussetzung für ihr Funktionieren." (Zeger 2008: 12) Und die Überwachung „funktioniert, weil die meisten freiwillig an ihr teilnehmen, oder sich die Vorteile, die sie bietet, nicht entgehen lassen wollen." (Kammerer 2008: 87) Überwachung trägt ein lockendes Element in sich, welches Vorteile suggeriert und den Tatbestand der Überwachung verschleiert. Wer Cookies im Browser aktiviert, kommt schneller zum Ergebnis. Wer auf Facebook seine/ihre Datenfreigabe lockert, bekommt bessere Positionierungen in den Newsfeeds seiner/ihrer Freunde. Wer die GPS-Daten des eigenen Smartphones für Dritte freigibt, bekommt relevantere Angebote, News und Wettervorhersagen. Wer seine/ihre E-Card mit dem Finanzamt verbindet, kommt schnell und unkompliziert zur Steuererklärung. Dass als Folge aber Unmengen privater und persönlicher Daten an externe Datensilos fließen und dort verknüpft und weiterverarbeitet werden, ist Nebensache. Generell, die Teilnahme am transparenten Social Web soll das Leben sozialer und besser machen. „Surveillance is not simply coercive and controlling. It is a matter of influence, persuasion and seduction." (Lyon 2001: 56)

Um dieses latente Überwachungsprinzip wissen auch die Vertreter der Post-Privacy-Theorie und fordern deshalb eine Entschleierung der Überwachenden. Der reine Tatbestand der Überwachung ist für sie kein Grund zur Sorge, denn „bedenklich ist Überwachung weniger aufgrund dessen, was jemand über jemand anderen weiß, als deswegen, was er mit diesem Wissen mit demjenigen anstellt." (Kammerer 2008: 89) Deshalb sollten Staat und Unter-

nehmen ihre BürgerInnen und KundInnen über diese Maßnahmen aufklären. „The wise company would survey users to make sure they understand what information is gathered about them, how and why it is used, and what control they have [...] to make sure that users are informed." (Jarvis 2011: 1888)

4.2c Überwachung für alle

In den Plädoyers der DatenschützerInnen für den Schutz der persönlichen, elektronischen Daten werden häufig düstere Zukunftsszenarien in Orwell's 1984er- oder Samjatins Wir-Manier nachgezeichnet (vgl. Kurz/Rieger 2011: 206ff), in welchen meist ein alles-überwachender Staat, eine Partei oder ein Weltkonzern im Mittelpunkt der Gesellschaft stehen. Die staatliche Überwachung, die etwa in Jewgeni Samjatins Roman „Wir" (Samjatin 1977) omnipräsent ist, manifestiert sich in etlichen, teilweise extremen Einschnitten in die Privatsphäre. Dort richtet sich das gesamte gesellschaftliche Leben nach einem panoptischen Gefüge, in welchem der „Einzige Staat" (Samjatin 1977: 19), „die starke Hand des Wohltäters und die scharfen Augen der Beschützer" (Samjatin 1977: 25) mit ihren drohnenartigen Flugzeugen für Recht und Ordnung sorgen. Die Menschen in diesem Staat haben keine Namen, sondern Nummern und leben in gläsernen Häusern ohne Geheimnisse voreinander. (Vgl. Samjatin 1977: 31) Selbst die Partnerwahl und Fortpflanzung sind streng reglementiert. Dieses Szenario vereint düstere Elemente aus dem Nationalsozialismus mit seiner Fortpflanzungsregulierung, dem Stalinismus mit Überwachung und Massenscoring und das im zynisch strahlenden Hochglanz einer Zukunftsutopie. Solche tiefgreifenden Einmischungen in das Privatleben unbescholtener BürgerInnen sind aus heutiger Sicht allerdings beängstigend und unvorstellbar, und dienen gerade deswegen - insbesondere anlässlich aktueller Bestrebungen nach mehr Überwachungs-

maßnahmen - immer wieder gerne als dunkle und unbedingt abzuwendende Zukunftsschau und Abschreckungsmethode. Was all diesen dystopischen Gesellschaftsformen - von der 'Brave New World' bis hin zum 'Einzigen Staat' - anhaftet, ist der Mangel an Souveränität und Selbstbestimmung ihrer BürgerInnen. Kaum jemand erhebt sich gegen das Joch der Big Brothers, Wohltäter und Beschützer.

Auch wenn sich DatenschützerInnen und Post-Privacy-BefürworterInnen in ihren Vorstellungen zum Schutz der Privatsphäre grundlegend unterscheiden, so sind sie sich hinsichtlich der oben geschilderten Überwachungsszenarien teilweise einig. Der einstimmige Kanon lautet zunächst: Die totale Top-Down-Überwachung wie bei Samjatin, Orwell und Konsorten ist nicht erstrebenswert. Zu einseitig seien die Machtverhältnisse, durch die Bindung aller Gewalten an eine übergeordnete Institution (vgl. Heller 2012: 1862).

Von hier an trennen sich aber die Wege. Wo DatenschützerInnen stur bleiben und weiterhin mit allen Mitteln ein Recht auf Anonymität im Netz einfordern und jegliche Überwachungsmaßnahme kritisieren und z.T. bekämpfen, sehen die VertreterInnen der Post-Privacy diesen Zug schon abgefahren. „Wenn eine wachsende Post-Privacy der Wirksamkeit persönlicher Anonymitäts-Taktiken letztlich den Boden entzieht, dann ist das halt so" (Heller 2011: online), lautet der trockene Kommentar aus dem Lager der „Post-Privacy-ioten" (Plomlompom 2011b: online). In diesem resignativ anmutenden Grundton lässt sich allerdings auch eine Chance verorten. Der Verzicht auf Anonymität, also eine Erleichterung und mögliche Ausweitung der Überwachungsmaßnahmen, kann - so die Vermutung - durchaus etwas Gutes an sich haben. Man macht sich als Individuum dadurch zu allen Seiten hin zwar angreifbarer, „das jedoch in einer Welt, in der sich verschiedene Wissensmächte gegenseitig im Zaum halten können. In der es keine unan-

greifbar einzige Wahrheit gibt, sondern so viele Wahrheiten wie Augen, Ohren und Köpfe. In der jede Machtanmaßung von allen nur denkbaren Seiten kritisch beäugt und auf Schwächen untersucht werden [...] kann." (Heller 2012: 1867)

Weniger Anonymität, mehr Transparenz und Offenheit relativieren also die Einseitigkeit der Macht der Überwacher. Hierin liegt auch einer der maßgeblichen Unterschiede zwischen klassischen Überwachungsgesellschaften und etwa der transparenten Gesellschaft von David Brin (1998). In Letzterer werden Macht und Machtmonopole hinterfragbarer und angreifbarer. Wer also mehr von sich preisgibt, sich über ein gesellschaftliches Problem öffentlich erhitzt und seine/ihre politische Meinung dazu kundtut, der/die findet in der transparenten Gesellschaft möglicherweise einfacher Gleichgesinnte, welche sodann in der Gemeinschaft gegen dieses Problem antreten. In einem geschlossenen Überwachungsregime würde ein derartiges Aufbegehren gegen ein staatliches Machtmonopol wohl sofort im Keim erstickt, resp. müssten Lösungsansätze, Revolutionen etc. im Stillen und Verborgenen ohne Rückhalt geplant werden.

Überwachung und - um es etwas drakonischer zu formulieren - Unterjochung sind in der utopisch-anmutenden Post-Privacy-Gesellschaft gar nicht mehr nötig, da ohnehin jede/r jede/n 'überwacht', so die Überlegung. Und zwar nicht im Sinne einer sich gegenseitig vor der Staatsgewalt denunzierenden Gemeinschaft. In der Transparenten Gesellschaft müssten, gemäß der Post-Privacy-Theorie, solche hierarchischen Unstimmigkeiten aufbrechen. „Bei Polizei und Verfassungsschutz schaut ein Gewaltmonopol von oben nach unten, vertikal, auf die Vielen. Die Transparente Gesellschaft dagegen stärkt die Horizontale gegenüber der Vertikalen: Die Vielen überwachen das Oben, aber auch einander gegenseitig nach links und rechts." (Hel-

ler 2012: 1799) In repressiven Überwachungsstaaten oder Diktaturen mit ihren Top-Down-Überwachungsprinzipien, mag es sein, dass Menschen unter diesem Obrigkeitsdruck in sich zusammenschrumpfen. Conformity is a classic survival reaction when people live in an ambience of terror and observation by unaccountable authorities." (Brin 1998: 154) Die Transparente Gesellschaft schließt dies aber aus. „Distrust and fatalism do not tend to dominate when transparency is reciprocal, nor when people retain a sense of participation and control. (Brin 1998: 154)

4.3 Achtung! Zu viel Privatheit kann schaden

Im folgenden versuche ich das Pferd von hinten aufzuzäumen und zu erläutern, welche Risiken ein Mehr an Privatheit birgt. Also noch einmal: Zu viel Privatheit kann schaden! Was zunächst nach einer radikaleren Post-Privacy-These klingt, wird auch aus einem anderen Lager konstatiert, wenn auch mit ganz anderen Hintergedanken. David Lyon, ein schottischer Soziologe, der seit den 80er-Jahren die sog. Surveillance Studies etabliert, sieht das auch so ähnlich. Ihn würde ich nicht unbedingt dem Lager der Post-Privacy-BefürworterInnen zuordnen.

4.3a Zu viel Privatheit macht überwachbar

Für Lyon verhält sich Privatheit zu Überwachung mehr als ein Komplement, denn als Korrektiv. Das soll so viel heißen wie: Der Rückzug in die Privatsphäre schützt das Individuum nicht vor Überwachung, sondern verstärkt diese sogar. (Vgl. Lyon 2001: 151) Lyon meint damit die Abspaltung des Individuums von der Gruppe. Ist der Mensch erst einmal allein, abgeschottet und eingemottet im vermeintlich sicheren Privatbunker, dann lässt er sich auch

leichter normieren und klassifizieren, eben überwachen. Die Flucht der Einzelnen in die jeweilige Privatheit, gleicht einer „Atomisierung der Gesellschaft und begünstigt dadurch gerade den überwachenden Blick" (Kammerer 2008: 88), den sie eigentlich verhindern wollte. Die Angst vor dem „Electronic Eye" (Lyon 2004: o.S.) und den technologischen Neuerungen mit all ihren integrierten Überwachunsoptionen, bewirken durch den Rückzug ins traute Heim, also nicht Kritik und Aufbegehren gegen die latenten ÜberwacherInnen, sondern Resignation. „Was benötigt wird, ist nicht der Rückzug in die eigenen vier Wände, sondern das In-die-Verantwortung-Nehmen der privaten oder staatlichen Datensammler, die verpflichtet werden müssten, Rechenschaft abzulegen über Verwaltung und Verarbeitung der von ihnen erhobenen Daten." (Kammerer 2008: 89)

Wenn also Kammerer und Lyon vom Risiko von zuviel Privatheit sprechen, dann ist damit neben dem Risiko vor zu viel räumlicher Privatheit, IMHO auch die erhöhte Sparsamkeit mit privaten Informationen, sprich auch das Risiko vor zu viel informationeller Privatheit gemeint. Der Rückzug aus Gesellschaft und aus Technik führt in diesem Szenario, wie geschildert, zur Isolierung und Atomisierung der Individuen. Darin sind die Individuen zwar keine offenen Bücher mehr, dafür sind sie gut verstaut, sortiert und katalogisiert. Sie sind einfacher zu überwachen und vor allem einfacher zu kontrollieren.

Denkt man nun etwa an das Überwachungsmonopol der Stasi in der DDR, so ist dieses Argument gar nicht so abwegig. Der Rückzug der Familien ins Private, die Bildung der Nischengesellschaft, stärkte damals die Autorität der Regierenden und ließ mögliche Aufstände erst gar nicht aufkeimen. Diese Form war eher ein isoliertes Nebeneinander ohne Öffentlichkeit, „über die man zu einem gemeinsamen kritischen Diskurs gelangen könnte." (Heller

2011: 1966) Jeff Jarvis, bekennender Transparenz-Verfechter, fragt sich deshalb: Hätte mehr Offenheit oder vielleicht sogar die verfrühte Einführung des Internet den Fall der Mauer beschleunigt oder erschwert? Wenn also die damals ersten Amiga-Computer bereits mit dem Internet und den Social-Media-Tools von heute gesegnet gewesen wären, „would dissidents have found one another sooner and realized that they had the critical mass - the safety in numbers - they needed to step out in public and bring down the government and its Wall? Or would the Stasi have hunted them down more efficiently?" (Jarvis 2011: 1052)

4.3b Zu viel Privatheit schafft Feinde

Post-Privacy-VertreterInnen verorten in einem verstärkten Rückzug in die Privatsphäre noch ein weiteres Risiko. Das Argument wirkt zunächst hanebüchen: Wer etwas vehement verbirgt, der macht alle anderen neugierig. „The person who claims the right to be alone, or even to keep things to herself, might meditate bad deeds or entertain bad thoughts, and no one would know…" (Jarvis 2011: 1826) Das Pochen auf Privatsphäre kann also auf Missgunst bei Mitmenschen stoßen, so die Argumentation. Auch Brin meint:

> We are, at our core, information pack rats and inveterate correlators. We hunger for news, facts, and rumors – especially when they are forbidden [or private, Anm. d. Verf.] […] If one kind of data acquisition is made illegal, you can be certain that someone will be doing it anyway on the sly." (Brin 1998: 80) Oder weiter: „When we enhance our own privacy, this may be seen by others as a sneaky attempt to keep them in the dark, a conspiratorial veil that might conceal threats to their liberty. (Brin 1998: 88)

Wer also, statt sich ‚per default' zu bekennen, etwas verbirgt, macht sich auch zum möglichen Opfer durch kriminelle Übergriffe auf seine/ihre Privatsphäre. Er/sie macht sich pauschal verdächtig, auch wenn das Geheimnis,

welches es zu verheimlichen gilt, per Gesetz geschützt ist (vgl. Brin 1998: 80). Deshalb lautet das Zauberwort der Post-PrivatistInnen zur Lösung des Dilemmas wieder einmal „Reciprocal Transparency." (Brin 1998: 81) Die gegenseitige Transparenz soll den Rückzug in die Privatsphäre überflüssig machen. Niemand muss mehr irgendetwas vor irgendwem verbergen, über alle Hierarchiestufen hinweg.

Wenn also beispielsweise die Mitarbeiter einer Discounter-Kette während ihrer Arbeit von Kameras überwacht werden, dann soll selbiges auch in der Manageretage geschehen und zwar für alle ersichtlich. Warum sollen die Manager nicht überwacht werden? Haben sie etwas zu verbergen? Überwachung in Unternehmen sei ohnehin ubiquitär geworden (vgl. Brin 1998: 81), deshalb wäre es, so die Logik, besser und fairer, die Tore der Überwachung zu öffnen und zwar in alle Richtungen. Der Ansatz lautet „not to close down information flows, but rather to compensate by opening them wider." (Brin 1998: 81).

Ein Mehr an Privatheit kann schützen, es kann aber auch isolieren und ein Individuum dadurch angreifbarer machen. Ein Mehr an Offenheit hingegen macht ein Individuum zunächst verwundbarer. Es kann in weiterer Folge aber auch zur raschen Konsolidierung und Verbreitung von Gedankengut führen und damit einen wichtigen Grundpfeiler von Demokratien untermauern resp. Revolutionen in Diktaturen herbeiführen.

Das Messer ist zweischneidig. Beide Optionen bergen Vor- und Nachteile oder anders formuliert: Chancen und Risiken. Nichts macht das deutlicher als die anhaltenden Grabenkämpfe zwischen den Post-Privacy-BefürworterInnen und den DatenschützerInnen. Etliche Argumente wurden auf die Wagschale gelegt. Die AkteurInnen in diesem ständigen Balanceakt zwischen

mehr Öffentlichkeit und mehr Privatsphäre, die BürgerInnen und UserInnen des Social Web, bekommen oft gar nichts von diesen Metadiskussionen mit, weil sie durch die Rahmenbedingungen der Post-Privacy möglicherweise längst zu Spielbällen der ubiquitären Technologie und der explodierenden Verdatung geworden sind.

> Our life, or at least the digital version of it, exists as rows and columns in massive databases somewhere in a 'cloud' of computers that we will never see, hear or reboot. We simply know that our information is recorded somewhere in the mysterious global network we know as the Internet and that as long as we click 'refresh' on our browsers, everything will be ok. And yet, this means that we do not fully have control or ownership over some of the most memorable recordings of ourselves. (Contreras 2013: 69)

Man ist versucht zu sagen: Wir sehen vor lauter Nebel die Wolke (Cloud) nicht mehr.

4.4 Scoring vs. Service

Unter den Begriff ‚Scoring' fasst man verschiedene Techniken zur Verdatung eines Individuums zusammen. Im Wortsinn versteht man unter Scoring den „Prozess des Zählens und des Einstufens von Zahlenwerten." (Kurz/Rieger 2011: 59) Die Technologie, insbesondere die Informationstechnologie, bietet heute einen schier unerschöpflichen Fundus an Tools und Mechanismen zur Aggregierung, Verknüpfung und Auswertung personenbezogener Daten zu unterschiedlichsten Zwecken. KritikerInnen sehen darin einen direkten Angriff auf die Menschenwürde (vgl. Zeger 2011: Interview) und eine Beschneidung der individuellen Freiheiten (vgl. Zeger 2008: 12ff). Post-Privacy-BefürworterInnen sehen das nicht so eng. Nach ihren Vorstellungen kann die zunehmende Verdatung von Individuen durchaus Vorteile bieten, insbesondere im Konnex der Empfehlungsindustrie der Social Networks und Shopping-Plattformen.

4.4a Scoring als Angriff auf die Menschenwürde

Kann man einen Menschen überhaupt in all seinen Wünschen und Zielen, in seiner Art und seinem Wesen auf einen kalkulier- und messbaren Datensatz reduzieren, ihn auswerten und vorhersagen? Gerade im Hinblick auf immer ausgefeiltere Algorithmen und Heuristiken scheint hier die Antwort verblüffend einfach: Ja… oder ist es doch nicht ganz so einfach? Kurz/Rieger verwenden im Kontext der statistischen Auswertung des Individuums den Begriff des „digitalen Schatten" (2011: 59, 197). Die Metapher hebt den Trugschluss hervor, wonach eben jenes digitalisierte Abbild eines Individuums, den wahren Menschen dahinter, in all seinen Facetten darstellen würde. Was aber jene Typisierungsalgorithmen tatsächlich über eine Person errechnen können, geht über ein digitales Schattenbild kaum hinaus. Es bleibt lediglich ein flacher, zweidimensionaler Umriss ohne Farbe, ohne Struktur, ein digitaler Schatten eben. Die Metapher lässt durchaus auch auf Platons Höhlengleichnis schließen. Dort werden die Schatten für wahr gehalten, wenngleich sie nur ein schemenhaftes Abbild der Realität liefern. „Heute werden die Datensätze für wahrer als die Wirklichkeit gehalten." (Zeger 2008: 16)

> Diese Persönlichkeitslandkarten sind mal schärfer, mal unschärfer, mal zeigen sie nur grobe Umrisse von Interessen, Meinungen und Begehren, oft jedoch sind sie erschreckend präzise und genau. Wie eine Landkarte können sie aber immer nur quantifizierbare, benennbare Eigenschaften aufzeigen. Hier gibt es eine Straße, einen Fluss, ein Dorf. Dass es dort wunderschön ist, zeigt die Landkarte nicht. Genausowenig wird hinter dem schubladisierten Persönlichkeitsabbild das verborgene einzigartige Menschenwesen sichtbar. (Kurz/Rieger 2011: 197)

Was ist also so schlimm daran, wenn uns Algorithmen nur schemenhaft ergründen können? So lauten in etwa die Stimmen aus dem Lager der Post-Privacy-VertreterInnen. Die Antwort der DatenschützerInnen: Die Algorith-

men werden immer besser! In einem Interview, welches wir, das Miio-Team im Rahmen des Dokumentarfilms ‚My Identity Is Open' mit dem Vorsitzenden der österreichischen Privacy-Organisation ARGE-Daten, Hans G. Zeger geführt haben, betonte auch dieser, dass das wahre Menschenbild mit algorithmisch erstellten Datenansammlungen kaum etwas zu tun hat. Er konstatiert:

> Wenn ich versuche jeden einzelnen Menschen in seiner Gesamtheit zu begreifen, seine Wünsche, seine Gefühle, seine Ziele, komme ich sehr schnell auf sehr komplexe Sachverhalte. […] Daher ist es für unsere Gesellschaft enorm wichtig, dass wir Menschen nicht in ihrer Gesamtheit wahrnehmen sondern immer in ganz bestimmten Rollen reduziert auf einen ganz bestimmten Sachverhalt. Genau das erreichen wir, indem wir Kategorien bilden und so aus den Menschen Datensätze machen. (Zeger 2011: Interview)

Die Antwort auf die oben gestellte Frage nach dem Umfang der Reduzier- und Kalkulierbarkeit eines Menschen muss also relativiert werden. Den Menschen in seiner Gesamtheit wahrzunehmen, hinter die Fassade zu sehen und ihn über mehr als nur algorithmisch erfassbare Parameter zu definieren, scheint sowohl heute als auch in absehbarer Zukunft technisch unmöglich. Doch darum scheint es den AkteurInnen und MotivatorInnen hinter der Datenauswertungsindustrie auch gar nicht zu gehen. Eine möglichst genaue aber gleichzeitig verkürzte Kategorisierung ihrer menschlichen Datensätze, um die kaum ergründeten wahren Menschen dahinter besser monetarisieren und steuern zu können, sind weitere mögliche Beweggründe der datenaggregierenden Konzerne und Staaten.

> Wir teilen die Menschen in wenige Kategorien ein, wie männlich, weiblich, Angestellte, Beamte, Arbeitslose, Sozialschmarotzer, Leistungsträger, Ausländer, Inländer etc. Und auf Grund dieser Kategorien können wir dann Entscheidungen treffen. Wir können Menschen dann als besonders wertvoll oder weniger wertvoll ansehen. (Zeger 2011: Interview)

Zegers Ansichten sind durchaus dystopisch. Ihm zu Folge durchdringt Scoring bereits die gesamte Gesellschaft. Ihre radikalste Ausformung findet diese Scoring-Gesellschaft in der „totalen Institution" (Zeger 2008: 34) Alle menschlichen Ziele und Eigenschaften werden darin in „berechenbare, strukturierte und kontrollierbare Daten" (Zeger 2008: 15) transformiert.

„Individualität und Identität werden durch Identifikation ersetzt." (Zeger 2008: 15) In dieser Gesellschaft tauschen Menschen ihre Persönlichkeit, ihre Wünsche und Vorlieben gegen einen Zahlenwert, die Identität gegen eine Nummer, so Zegers Ansatz. Das Problem liege überdies darin, dass aus der schattenhaften Reduktion eines Menschen, gleichzeitig folgenreiche Schlüsse gezogen werden und zu enormen Ungerechtigkeiten im Scoring-System führen können. Was letztlich zu Aufruhr und Gegenwehr führen sollte, sei in der Passivität dieser Antimoderne gar nicht mehr möglich, da die „Ausgestaltung und Ausübung individueller Rechte zunehmend als gesellschaftliche Belastung empfunden werden." (Zeger 2008: 12) Durch den zwanghaften Zug, ja eine regelrechte „Lust an totaler Kontrolle" (Zeger 2008: o.S.) kann sich diese Kontrollgesellschaft auch ständig selbst reproduzieren.

Kein Ausweg also. In Zegers Auffassung schwingt neben der dystopisch anmutenden Grundstimmung auch ein Hauch Resignation und Misanthropie mit. „Was wir zu datenbesetzten Objekten reduzieren, dem fehlen Eigenverantwortung und vernünftiges Handeln, es muss kontrolliert, gesteuert werden." (Zeger 2008: 16) Und so wird Kontrolle zum „Ausdruck des geringen eigenen Selbstwertgefühls." (Zeger 2008: 13)

Der Mensch, einmal auf einen Datensatz reduziert, und damit um seine Menschenwürde beraubt, hat also kaum eine Möglichkeit, dem ‚System' zu entkommen. In dieser ideologiekritischen Sichtweise, macht Scoring den

Menschen nicht nur zum/zur gläsernen BürgerIn. Es schafft gleichzeitig auch gläserne Mauern um die BürgerInnen herum. Die Kontrollmechanismen, die dahinter stecken sind so alltäglich und subtil, dass sie den Betroffenen quasi gar nicht auffallen.

4.4b Scoring als Chance

Nun wieder zur Zweischneidigkeit der Klinge. Für die einen ist Scoring Teufelswerk und eine Verletzung der Menschenwürde, für die anderen stellt Scoring resp. die zunehmende Verdatung aller Bereiche der Gesellschaft, eine Chance dar. OffenheitsbefürworterInnen betrachten das erhöhte Datenaufkommen in all seiner Konsequenz, auch weniger von einer Macht- und Kontroll-motivierten Perspektive aus. Ihre Perspektive ist eine pragmatische. In der Verdatung sehen sie eine Serviceleistung. „Amazon [...] builds a profile of my interests and tastes, and tries to sell me what I'll want. Amazon.com has also begun telling me what is popular with my Facebook friends. No department store ever did all that for me." (Jarvis 2011: 768) Was da im Hintergrund passiert ist mir egal, Hauptsache es bringt mich weiter. Die Daten-Tauschgeschäfte zwischen Konzernen und Privatpersonen - also Datenfreigabe gegen gezieltere Werbung, bessere Empfehlungen etc. - haben so gesehen auch ihr Gutes. Zugleich suggeriert diese Praxis dem Service-verwöhnten Individuum ein erhöhtes Aufmerksamkeitsvolumen. Jeder Kauf, jede Buchung, jede Terminvereinbarung, jedes Onlinespielergebnis, jeder Klick erzeugen Scoring-Parameter, welche den Unternehmen nicht nur Prognose- und Zuordnungsmöglichkeiten eröffnen, sondern den betroffenen KundInnen gleichermaßen neue Aufmerksamkeitskanäle schaffen. Alles kann schließlich auch via Facebook geshared werden. Scoring optimiert quasi Verkaufsprozesse, steigert die Trefferquote bei Empfehlungen und ver-

bessert die Kundenzufriedenheit. Am Ende sind alle happy. Was ich hier zynisch kommentiere, legt Brin bereits vor 15 Jahren auf die Waagschale. Nachdem er die datenaggregierende, -hortende und -weiterverarbeitende Praxis der ‚bösen' Großkonzerne und Internet-Granden ausführlich anhand von Beispielen darlegt, stellt er die Frage an den/die LeserIn: „How much of the above do you find objectionable? How much of your objection is due to real, tangible harm - and how much of it is on principle?" (Brin 1998: 57) Eine berechtigte oder eine naive Frage? Lass sie doch Daten sammeln, zählen, kombinieren und auswerten. Macht uns doch nichts aus. Im Gegenteil: Es bringt uns sogar Vorteile. Nach dem Motto: ‚Was sich gut anfühlt, ist gut', werden Scoring-Methoden nicht nur übersehen, sondern auch gerne angenommen, quasi blind akzeptiert. Denkt man die Idee der Post-Privacy von mehr Transparenz aber konsequent durch, dann dürfte Scoring, egal ob in der Medizin, der Finanzbranche oder im täglichen Konsum, nicht verschleiert passieren. Die Funktionsmechanismen und ihre Reichweite müssten offengelegt werden.

Geht man von der Annahme aus, in einer utopischen Post-Privacy würden gar jene Scoring-Prozesse offengelegt, die eigentlich der Monetarisierung und Überwachung der Individuen dienen sollten, so wäre dies wahrscheinlich die bessere Option als die jetzige, in welcher das Individuum den Verdatungsprozessen blind ausgeliefert ist. Schüfe man dazu noch offene Schnittstellen zur Mitgestaltung der Scoring-Algorithmen, so könnten Fehler, welche z.B. für Ungerechtigkeiten im Scoring-System sorgen, schneller behoben werden. Generell könnten Ungleichgewichte, durch die offene Struktur, rasch ausgemacht und ggf. angeprangert werden. Transparentes Scoring ist allerdings auch nur ein Kompromiss, kein Korrektiv, sondern das erträglichere Übel, da Scoring an sich in der transparenten Gesellschaft ja nicht abgeschafft wird. Die Haltung bleibt resignativ. Es gilt auch hier die

Maxime der Post-Privacy: Transparentes Scoring ist besser als Scoring. Was man den Zahlenspielen unabhängig der Art der Gesellschaftsform, in welcher sie eingebettet sind, zu Gute halten kann, ist, dass sie gewissermaßen farbenblind sind.

> In their supposedly color-blind impartiality, such ratings have actually been used to help quash racial and other kinds of discrimination." (Brin 1998: 59) Wo Menschen früher Aber: „Yet the scorers employed by these private companies keep their methods secret, thereby making it hard to spot errors or patterns of bias. (Brin 1998: 59)

4.5 Verlust über die eigene Datenhoheit

Geht man von der Kant'schen Idee[12] aus, dass der Mensch wirklich nur in freier Selbstbestimmung seiner Würde gerecht werden kann (zit. n. Beck u.a. 1995: 201), so kann man daraus schließen, dass die Demokratie mit all ihren Freiheiten, die Gesellschaft in der Bewahrungsmoral ihrer Würde, ein ganzes Stück nach vorne katapultiert hat. Betrachtet man vor diesem Hintergrund die Situation um die informationelle Selbstbestimmung, damit ist die Entscheidungsgewalt über all jene personenbezogenen Daten, die über einen Menschen kursieren gemeint, so bleibt von Kants Idee nicht mehr viel übrig. So heißt es etwa im Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz von 1983:

> Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen seiner Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen
> und zu entscheiden. (grundrechteschutz.de: online)

[12] Kants Beispiel dient hier eher als stark verkürztes und veranschaulichendes Axiom und soll hier nicht näher diskutiert werden.

Nicht zuletzt deswegen stemmen sich Kurz und Rieger in ihrem „Wegweiser zur digitalen Mündigkeit" (2011), vehement gegen die Post-Privacy-VerfechterInnen, welche wiederum in der informationellen Selbstbestimmung einen Angriff auf die Redefreiheit sehen (vgl. Plomlompom 2011a: online). Sie sehen hinter dem Kanon der Post-Privacy ein enormes Gefahrenpotenzial. Hier würde zum Einen „der Eindruck der Unausweichlichkeit erweckt. Die technologische Entwicklung und der einhergehende Verlust der Datenkontrolle wird als alternativlos dargestellt. […] Privatsphäre ist etwas von gestern." (Kurz/Rieger 2011: 101) Zum anderen entstehe so der weitläufige Glaube, dass ein Aufbegehren gegen die dubiosen Machenschaften der Datensammler gar nicht lohnen würde, da alle digitalen Ichs und all die dazugehörigen Datenschnipsel ohnehin längst in den Datenbanken von Amazon, Facebook, Google und Co. liegen würden. Da grenze es schon an Naivität, wenn man heute noch glaubt, man könne über seinen digitalen Abriss noch voll verfügen.

Tatsächlich scheint es kaum Konzepte zu geben, die mögliche Eindämmungsoptionen des überbordenden Kontrollverlustes aufzeigen, einmal von der strikten Datenaskese abgesehen, welche aus heutiger Sicht wohl das Leben (inklusive Geburt) in einer Höhle voraussetzen würde. Wer heute am Leben im Netz mit all seinen Vorzügen teilhaben möchte - und auch dies wird in Anbetracht der Dynamiken unserer Bekenntnis- und Partizipationskultur immer mehr zum Zwang denn zur Option (wer möchte schon in einer Höhle leben) - der/die muss davon ausgehen, dass sich ein Gros der dabei hinterlassenen Datenspuren seiner/ihrer Kontrolle entzieht. „Sind unsere Daten bereits irgendwo gespeichert, dann haben wir die Kontrolle über sie verloren - egal, was die versprechen, denen wir sie anvertraut haben." (Heller 2011: 323) Man ist geneigt, dieser Feststellung, kritiklos zuzustimmen. Der Verlust über die eigene Datenhoheit lässt sich wohl eher als Gegebenheit,

denn als Vor- oder Nachteil, Chance oder Risiko einer Post-Privacy-Kultur deuten. Jede/r der/die schon einmal versucht hat bei Google anzurufen, um einen Eintrag löschen zu lassen, weiß dass dies ein Kampf gegen Windmühlen ist.

4.6 Autonomieverlust über die Selbstdarstellung

Autonomieverlust klingt immer drastisch. Im Zusammenhang mit der informationellen Selbstbestimmung kann ein solcher Verlust, wie bereits dargelegt, enorme Auswirkungen auf das Verständnis von Privatsphäre haben. Doch wie steht es um den Verlust der Autonomie über die eigene Selbstdarstellung? Geht man davon aus, dass die Mehrzahl der sozialen Interaktionen mittlerweile im Internet, über diverse Social Web Tools passieren, so kann man daraus herleiten, dass sich bestimmte Verhaltensweisen, die eine soziale Interaktion im realen Umfeld prägen, auch ins Netz verlagern können. Das betrifft insbesondere auch jegliche Praxis und Technik der Selbstdarstellung.

Nach Goffmans Bühnentheorie (2003) kann man sich den Alltag und das gesellschaftliche Leben wie ein große Bühne vorstellen auf welcher jede/r BürgerIn gleichermaßen die Rolle des/der Schauspielers/in als auch des/der Zusehers/in einnimmt. Man bemüht sich einerseits also darzustellen, um dem weitläufig akzeptierten Fremdbild zu entsprechen, oder auch nicht und beobachtet/beurteilt gleichzeitig jede Interaktion im Umfeld. In einer vollkommen transparenten Gesellschaft hätte man keine Kontrolle mehr über das Schauspiel auf dieser Bühne. Die Selbstdarstellung als konstitutives Tool wäre in der transparenten Gesellschaft um ihre Grundlage, ihre Notwendigkeit beraubt. Niemand muss oder vielmehr kann sich mehr verstellen, wenn bereits alles über ihn/sie in Erfahrung gebracht werden kann. Die Doppelrol-

le des/der Darstellers/in und Zusehers/in wird reduziert auf die alleinige Rolle des/der Zusehers/in. Jede/r ist wie er/sie ist und schaut den anderen dabei zu.

Der Hund liegt in dieser Annahme nicht tief begraben. Ein paar Beispiele aus dem Seelenleben eines Menschen, helfen beim ausbuddeln. Wie etwa möchte man in einer Welt der uneingeschränkten, reziproken Transparenz mit Scham umgehen? Dass dieses Gefühl der peinlichen Berührtheit sich durch ein zunehmendes Maß an gegenseitiger Offenheit einfach wegrationalisieren lässt, kann man in der heutigen Norm als abwegiges Wunschdenken deuten. Technologien und Gesellschaftspraktiken, welche die Zugänglichkeit und Öffnung von Identitäten fördern, wie etwas das nicht mehr ganz so futuristische Miio-Device, könnten aus dem leicht zurückhaltenden Mauerblümchen eine/n waschechte/n SozialphobikerIn machen. So wird der/die vermeintlich gleichgestellte ZuseherIn sehr schnell wieder zum/zur ungewollten DarstellerIn auf der Bühne, „angestarrt von einer kritischen Öffentlichkeit, ohne den Text zu wissen oder seine Rolle adäquat spielen zu können. Im nächsten Moment droht das Publikum, einen mit Buhrufen und Pfiffen sozial zu vernichten. Scheinbarer Ausweg ist der soziale Rückzug: Weg von der imaginierten Bühne, ins soziale Off der oftmals generalisierten Vermeidung." (Hilgers 2013: 82) Das wirft einige Fragen auf: Wie soll man in der Welt der Miio-Devices eine/n SozialphobikerIn therapieren können? Wie geht man mit Scham um? Schafft man sie ab?

> Der Schutz informationeller Privatheit ist deshalb so wichtig für Personen, weil es für ihr Selbstverständnis als autonome Personen konstitutiv ist, (in ihnen bekannten Grenzen) Kontrolle über ihre Selbstdarstellung zu haben, also Kontrolle darüber, wie sie sich wem gegenüber in welchen Kontexten präsentieren, inszenieren, geben wollen, als welche sie sich in welchen Kontexten verstehen und wie sie verstanden werden wollen, darum also auch, wie sie in welchen Kontexten handeln wollen. Zur Erklärung, was mit der Verletzung informationeller Privatheit verletzt wird, greife ich also zurück auf die Begriffe von Frei-

> heit und Autonomie und knüpfe damit an philosophische Theorien an, aber auch etwa an Entscheidungen des Bundesverfassungsgerichts, die beide einen engen Zusammenhang zwischen der Verletzung informationeller Privatheit und der Möglichkeit individueller Freiheit sehen. (Rössler 2001: 23)

4.7 Masken fallen lassen!

Das Problem des Autonomieverlustes über die Selbstdarstellung löst sich nach Ansicht der Post-PrivatistInnen in einer transparenten Gesellschaft, ganz von selbst. Privatsphäre gibt Menschen die Möglichkeit des Rückzugs, „the space and freedom to create and experiment." (Rossiter/Konvitz 1957: 15) Sie erlaubt es ihnen ihre Masken des Alltags zur Seite zu legen, um für einen Moment sie selbst sein zu können (vgl. Westin 1970: 34f). Das legt nahe, dass der Mensch nur im Rückzug in die Privatsphäre ganz authentisch sein könne. Dies aber wäre ein Armutszeugnis für zwischenmenschlichen Beziehungen, müsste man sich in der Öffentlichkeit ständig verstellen (vgl. Jarvis 2011: 1778).

In der Post-Privacy wird dieses Modell radikal umgedreht. Dort sollte man die Masken der Selbstdarstellung gar nicht erst aufsetzen. Auch Freiheiten für Kreativität und Experimente böten sich in der Öffentlichkeit zur Genüge. Authentizität und Transparenz kann schließlich auch Beziehungen und gegenseitige Solidarität fördern. Und man hätte ohnehin nichts zu befürchten. Das glaubte auch David Brin.

> As people feel more secure in general on the Net, they will become accustomed to seeing their words recorded and replayed. They will no longer feel uncomfortable being on display, since everyone around them is on display too. (Brin 1998: 157)

4.8 Beziehungen, Toleranz und Solidarität

Aus einer kritischen Betrachtungsweise, kann Post-Privacy zunächst als das Gegenteil von Solidaritäts- und Beziehungs-fördernd gedeutet werden. Durch die Verdatung der Individuen treibt sie einen Keil zwischen die Subjekte. Einzeln und heruntergebrochen auf einen Datensatz, gefangen in ihrer Welt der Sozialen Medien, in der es vielleicht doch nur um Aufmerksamkeit geht, sind diese leichter zu steuern. Isoliert und trotzdem im Glauben, Teil eines großen, vernetzten Ganzen zu sein, kommen die Individuen so gar nicht erst auf die Idee, sich zu solidarisieren und zu erheben.

Aus einer pragmatischeren Sichtweise, kann Post Privacy aber durchaus Dynamiken der Solidarisierung und Konsolidierung fördern. Das augenscheinlichste Argument für mehr Offenheit und Transparenz liefert die Konnektivität des Social Web, welche es den Individuen erlaubt, miteinander in Verbindung zu treten. „The internet has changed the infrastructure of relationships." (Jarvis 2011: 794) Wer sich auf Facebook öffnet, findet im Handumdrehen alte SchulfreundInnen und Bekannte und kann sich mit ihnen in Verbindung setzen, Beziehungen aufbauen. Die Bereitschaft offener zu sein und mehr von sich preiszugeben, kann außerdem dabei helfen Gleichgesinnte zu finden. Das 'Ugol's Law', ein nach Harry Ugol benanntes Gesetz und erstmals in einem Forum für Sadomaso und Bondage erwähnt, besagt, dass man mit seinen Vorlieben nie allein ist, egal wie weltfremd und kurios sie auch erscheinen mögen (vgl. Jander 2001: online). „For any given kink, either nobody does it or more than one person does it." (Ugol 1996: online, zit. n. Jander 2001: online) Andersartigkeit, Obskurität und Verschrobenheit sind demnach in der Welt der Konnektivität, kein Grund mehr in Scham und Abkapselung zu leben. Man ist ja schließlich nicht allein und das Internet hilft einem/einer bei der Suche nach dem passenden Gegenstück. Diese

Art der Zusammenführung ermöglicht, wenn man Post-Privacy radikal zu Ende denkt, vielleicht sogar eine Überwindung der Scham. Finden sich nur genügend Andersartige, dann fällt der Weg in die Öffentlichkeit auch leichter. Was landläufig vielleicht als Perversion erachtet wurde, kann durch Solidarisierungsprozesse der Post-Privacy, als etwas alltägliches, normales, schlicht gegebenes enttarnt werden. In diesem Kontext fördert Post-Privacy die Überwindung festgefahrener, gesellschaftlicher Stigmen und schafft damit einen fruchtbaren Boden für mehr Toleranz. Jarvis hat diese Macht der Öffentlichkeit anhand der massenhaften ‚Outings' von Homosexuellen aufgezeigt, welche sich damit gegen die herkömmliche Auffassung von Sexualität erhoben. „Secrecy did not give gays control over their lives; it granted control to the bigots who forced their norms on others. The solution for gays was to come out, to be public, to show pride, to gather in solidarity and in strength, and to defy society to disapprove." (Jarvis 2011: 972) Vor diesem Hintergrund, wird die Propagierung zu mehr Vorsicht und Zurückhaltung im Netz, zur Einforderung der Privatsphäre, als antiquiert und veränderungsfeindlich denunziert (vgl. Solove 2008: 95).

Wie ich bereits angedeutet habe, können die Tools der Post-Privacy auch dabei behilflich sein, eine kritische Masse zu bilden, um ganze Revolutionen vom Zaum zu brechen. Die ständige Vernetztheit durch internetfähige Smartphones und Services wie Twitter, macht es möglich, selbige auch zu koordinieren. Post-Privacy konsolidiert gewissermaßen die Horizontale (BürgerInnen) gegenüber der Vertikalen (Herrschende) und kann so gewisse Machtassymetrien ausgleichen. Allerdings kann der Schuss auch nach hinten losgehen. Machen sich die Auflehnenden erst einmal erkennbar, so können die Machthabenden, beispielsweise in repressiven Regimes, die selben Tools und Informationspools nutzen, um die Meuterei niederzuschlagen. Nutzen die Machthabenden darüber hinaus noch ihre Position, um im Revo-

lutionszustand die offenen Kanäle zu zensieren resp. lahm zu legen, dann wird das Post-Privacy-Prinzip der reziproken Transparenz ausgehebelt und fällt zurück in ein Muster der totalitär-anmutenden Top-Down-Überwachung.

4.9 Optimierung durch Wissen

Durch eine rigide „Open Data Policy" (Civic Commons 2013: online) kann mittels Transparenz, jede Menge neues Wissen angehäuft werden, welches dazu genutzt werden kann, gesellschaftliche Lebensbereiche zu optimieren. Im Rahmen des Projekts ‚Google Flu Trend Estimates' kombiniert Google offizielle und öffentliche Grippedaten von Gesundheitsinstituten mit den eigenen Grippe-Suchanfragen und kann so Schätzungen über die Häufigkeit von Grippeerkrankungen in einem bestimmten geografischen Gebiet, zu einem bestimmten Zeitraum vornehmen (vgl. Google Flutrends 2013: online). DatenschützerInnen mögen dabei erschaudern, doch denkt man diese Praxis weiter, können in der Kombination von Gesundheitsdaten und privaten Suchanfragen, Pandemien möglicherweise rechtzeitig erkannt und eingedämmt werden. In Österreich war die Wahrscheinlichkeit an einer Grippe zu erkranken in diesem Jahr am 17. Februar am höchsten.

Öffnen Regierungen ihre Datenpools, dann multipliziert sich auch die Anzahl der Augen, die das politische Geschehen kritisch beobachten. Wieder kommt die reziproke Transparenz ins Spiel. Ungefiltert können BürgerInnen, Journalisten und Wissenschaftler Einsicht in Regierungsdaten nehmen und gleichzeitig die Machenschaften der Regierenden verfolgen. Mögliche Skandale zu vertuschen würde in diesem umgekehrten Panopticon zunehmend schwieriger. Langwierige und kostspielige Aufklärungsprozesse und U-Ausschüsse

könnten erspart bleiben. „Citizens seem to know almost instinctively that it is better to shine too much light than too little." (Brin 1998: 87)

Beispielgebend dafür, wie man durch Transparenz, ganz persönliche Lebensbereiche optimieren kann, steht etwa die AktivistInnen-Gruppe um ‚The Quantified Self.' „A place for people interested in self-tracking to gather, share knowledge and experiences, and discover resources." (quantifiedself 2013: online) In teilweise penibelster Akribie, erstellen die Mitglieder Protokolle ganz alltäglicher Tätigkeiten, veröffentlichen sie und verschaffen sich und anderen damit einen Blick auf sich selbst von außen. Diese Art der persönlichen Verdatung kann etwa genutzt werden, um Ernährungs-, Sport- oder Schlafgewohnheiten zu protokollieren, auszuwerten und schließlich daraus Schlüsse zu ziehen. Durch die gewonnenen Erkenntnisse können so etwa missliche Gewohnheiten eruiert und korrigiert werden. Diese Selbstquantifizierung macht es möglich, alle verdatbaren Lebensbereiche zu kalibrieren und optimieren, „die Datenintelligenzen des Netzes direkt ans eigene Leben anzuschließen, ihm dienstbar zu machen." (Heller 2011: 964)

Fazit

Nach diesem Abriss zur Post-Privacy, über ihren Entstehungskontext und ihre BefürworterInnen, über die Vor- und Nachteile sowie Trugschlüsse die man aus ihr ziehen kann, möchte ich die anfangs gestellte Forschungsfrage beantworten.

Welche gesellschaftlichen Chancen und Risiken ergeben sich aus einer aufkeimenden Transparenzkultur?

In Kapitel 3 und 4 bin ich auf die Chancen und Risiken der Post-Privacy eingegangen und konnte einige Aspekte klären. Die Antwort auf die Frage ist aber nicht eindeutig, zumal das Verhältnis von Chance-Risiko immer genau abgewogen werden muss. Was für die einen ein Vorteil, eine Chance ist, birgt für die anderen wiederum Gefahren. Aufgefallen ist mir, dass Kritik an der Post-Privacy häufig mit Ideologiekritik zusammenhängt. Demnach diene Post-Privacy einer latenten Unterjochung der Individuen und verstärke lediglich die Machtverhältnisse der Herrschenden (vgl. Kurz/Rieger 2011, Reichert 2008, Krotz 2001). Die Seite der BefürworterInnen hingegen wählt häufig pragmatische und technikdeterministische Argumentationen.

Post-Privacy und die Technologie, die sie hervorbringt, kann die Gesellschaft solidarisieren, zusammenbringen und toleranter machen. Wenn jede/r alles über jede/n weiß, hat schließlich niemand mehr etwas zu befürchten, muss sich niemand schämen, denn dann sind alle gleich nackt. Post-Privacy kann ein Individuum mit ihren Tools aber auch isolieren und angreifbarer machen. Wenn ich private Details über eine Person zu deren Nachteil veröffentliche, weil ich ja darauf zugreifen kann, dann hat das mit Toleranz wenig zu tun. Einige Mitglieder der Gesellschaft, können durch Post-Privacy-Taktiken

leicht zu Zielscheiben werden. Kranke, Übergewichtige, Homosexuelle, die ihre Lebensgeschichte nicht mit der Welt teilen möchten, können im Zeitalter der Transparenz ohne große Schwierigkeiten enttarnt und je nach Absicht, bloßgestellt werden.

Scoring, die Verdatung und Einordnung eines Menschen in ein Bewertungssystem, stellt für viele DatenschützerInnen einen direkten Angriff auf die Menschenwürde dar. Wird ein Mensch erst einmal auf eine Nummer reduziert, dann bleibt von seiner Würde nicht mehr viel übrig. Er büst Freiheiten ein und ist leichter steuerbar. Andersrum kann Scoring, also die Auslagerung von Bewertungsmechanismen auf Algorithmen, wiederum menschliche Fehler ausgleichen. Bei der Kreditvergabe müssen vom Score Eigenschaften wie Hautfarbe oder Herkunft ignoriert werden, während ein Bankberater immer auch ein klein wenig nach Gutdünken entscheiden kann.

Post-Privacy öffnet der Überwachung Tür und Tor. Jede/r mit Internetzugang und Smartphone kann heute auf Schritt und Tritt überwacht werden, sei es vom Staat, von privaten Institutionen oder auch nur von seinen/ihren Mitmenschen. Ein Mehr an Daten weckt ständig neue Begehrlichkeiten. Mit der zunehmenden und teils freiwilligen Verdatung, können ganz neue Überwachungsmaßnahmen etabliert werden, die immer ausgefeilter und tiefschürfender werden. Andererseits kann Überwachung, wenn sie konsequent in alle Richtungen ausgeweitet wird, für alle von Nutzen sein. Der Staat schützt mit seinen Überwachungsmaßnahmen die BürgerInnen vor Kriminellen und TerroristInnen. Dabei wird er durch die Tools der Post-Privacy sogar unterstützt, wie der Fall der Bostoner Bombenattentäter jüngst gezeigt hat. Umgekehrt überwachen die BürgerInnen den Staat, welcher in der Post-Privacy auch alles offen legen muss. Der Ansatz ist zwar resignativ, aber zumindest pragmatisch. „Wenn die Überwachung schon total wird und alle

erfasst, dann soll sie wenigstens auch allen zur Verfügung stehen." (Heller 2011: 1778) Auf dieser Idee, der Reziprozität der Transparenz, beruht letztlich das Konzept der Post-Privacy, welches der Gesellschaft nie dagewesene Möglichkeiten eröffnen soll.

> Despite uncountable flaws in our contemporary neo-Western wolrd, there has never been a major urban society in which individuals of all social classes had more freedom than we do today. [...] The one factor making this possible has been reciprocity of information flow. (Brin 1998: 87)

Die Liste der Chancen und Risiken, die jeweils eigentlich beides sind, kann noch ewig fortgeführt werden. Und je nach Lager findet sich bestimmt immer wieder ein Argument für die eine oder andere Seite.

Die Zukunft muss also nicht zwingend eine düstere sein, auch wenn sie etliche Technologien hervorbringen wird, die manch eine/n aus heutiger Sicht erschaudern lassen. Das Miio-Device als Super-Überwachungstool für jedermann, ist dabei längst nicht der Weisheit letzter Schluss. Ein Projekt wie ‚Google Glass', als Brillenerweiterung fürs Smartphone, war zu Beginn unserer Projektplanung vor wenigen Jahren, noch reißerische Zukunftsmusik. In einem Jahr könnte die smarte Hightech-Brille aber schon über die Ladentische gehen. Der technologische Fortschritt lässt sich nicht aufhalten. Aber gilt genau das auch für den Verlust der Privatsphäre? Ist dieser auch nicht mehr zu stoppen?

Nach dem Abschluss dieser Arbeit, kann ich getrost sagen: Leider ja! Privatsphäre wird zwar immer ihre Nischen bewahren, im Netz allerdings, mit seiner Konnektivität, wird sie zunehmend von allen Seiten bedrängt. Je tiefer die Vernetzung in all unsere Lebensbereiche eindringt, auch in bislang private Bereiche, umso stärker zerfranst unsere Vorstellung von Privatsphäre.

„Es war in der Geschichte der Menschheit bei der Entwicklung neuer Technik immer so, dass natürlich wir darüber bestimmen, wie sie in Zukunft eingesetzt wird." (Kurz 2011: Interview) Es wird aber in Zukunft nicht nur darum gehen, wie neue Technologien angenommen und in den Alltag integriert werden. Es wird genauso von Belang sein - um nicht wieder in einen Technikdeterminismus zu verfallen - wie die Konzeption und Ausgestaltung der Technologien erfolgt, so dass sie ein ausgeglichenes Maß an Freiheit und Privatsphäre berücksichtigen. „Privacy by design" (Hustinx 2011: Interview) könnte ein Ansatz sein. Demnach wird Technik so gebaut, und integriert, dass sie keine Gefahr für die Privatsphäre darstellt. Das ist allerdings leichter gesagt als getan, denn der Wunsch nach mehr technologischer Freiheit, scheint den Wunsch nach mehr Datenschutz und Privatsphäre eindeutig zu überwiegen. Das zeigt auch ein Blick in die Vergangenheit. Zweifel an der Eisenbahn (Überforderung durch Geschwindigkeit), der Druckerpresse (Informationsflut), der Fotografie (Privatsphäre) und dem Internet (Privatsphäre), konnten die rasche Verbreitung der technologischen Neuheiten nie unterbinden.

„Open by default, secret by necessity" (Jarvis 2011: 3278) ist der andere Weg, der den die Post-Privacy einschlägt. Transparenz als Standard und Privatsphäre nur dort wo sie wirklich nötig ist. Es scheint, als ob dieser Pfad zum Königsweg erhoben wurde. In diesem Szenario verschwindet Privatsphäre nicht, aber sie wird weniger und anders. Die Grenzen zwischen Privatsphäre und Öffentlichkeit lösen sich mehr und mehr auf. D.h. aber nicht, dass Privatsphäre deswegen nicht auch in gewisser Weise behütet werden müsste. Wenn also Technik die Privatsphäre nicht mehr schützt, dann müssen es die Menschen im Umgang miteinander tun. Wenn ich einem Freund ein Geheimnis erzähle, und dieser es kurzerhand auf Facebook verbreitet, dann liegt das Problem nicht nur an der Technologie von Facebook, sondern wohl

eher an der Wahl des Freundes. Der Schutz der Privatsphäre dient in diesem Kontext eher der Symptombekämpfung. Das tiefer liegende Problem, bleibt unbehoben. Ein weiteres Beispiel: Wenn ich im uferlosen Datengewimmel der Post-Privacy etwas aufschnappe, was nicht für meine Augen bestimmt war, dann sollte ich vielleicht wegsehen[13], anstatt es unbedacht weiterzuverbreiten. Reziproke Transparenz erfordert auch reziproke Verantwortung. Möglicherweise liegt darin der Schlüssel. Ein Regelbuch oder Ethos der Post-Privacy wäre anzustreben.

[13] Das eigenständige Herausfiltern von Informationen, nach dem Prinzip der "Filtersouveränität" (Seemann 2011: online), zügelt das Hinsehen und nicht das Posten. Der Grundsatz: Selbstzensur statt Zensur.

Literaturverzeichnis

Monographien, Sammelbände und Fachjournale

Abels, Heinz (2006): Identität. Wiesbaden: VS-Verlag.

Agres, Philip E./Rotenberg, Marc (1998): Technology and Privacy: The new Landscape. Cambridge: MIT Press.

Ariès, Philippe (1986): Zu einer Geschichte des privaten Lebens. In: Ariès, Philippe/Chartier, Roger (Hg.): Geschichte des privaten Lebens. Von der Renaissance zur Aufklärung. Frankfurt: S. Fischer.

Bauman, Zygmunt (1992): Moderne und Ambivalenz. Das Ende der Eindeutigkeit. Hamburg: Junius.

Beck, Ulrich (1995): Eigenes Leben: Ausflüge in Die Unbekannte Gesellschaft, in Der Wir Leben. München: C.H.Beck.

Clarke, Roger (1988): Information Technology and Dataveillance. In: Communications of the ACM 31. Jg., H. 5, S. 498-512.

Contreras, Esteban (2013): Social State: Thoughts, Stats and Stories about the State of Social Media in 2013. Ebook.

Duby, Georges (1990): Private Macht, öffentliche Macht. In: Duby, Georges (Hg.): Geschichte des privaten Lebens. Vom Feudalzeitalter zu Renaissance. Frankfurt: S. Fischer.

Ezra Park, Robert (1950): Race and Culture. Glenoce: The Free Press.

Goffman, Erving (2003): Wir alle spielen Theater. Die Selbstdarstellung im Alltag. München: Piper.

Hall, Catherine (1987): Trautes Heim. In: Perrot, Michelle (Hg.): Geschichte des privaten Lebens. Von der Revolution zum Großen Krieg. Frankfurt: S. Fischer.

Heller, Christian (2011): Post-Privacy. Prima Leben ohne Privatsphäre. Ebook.

Hilgers, Micha (2013): Scham. Gesichter eines Affekts. Göttingen: V&R.

Jarvis, Jeff (2011): Public Parts. How Sharing in the Digital Age improves the Way we Work and Live. Ebook.

Krotz, Friedrich (2001): Die Mediatisierung des kommunikativen Handelns. Der Wandel von Alltag und sozialen Beziehungen, Kultur und Gesellschaft durch die Medien. Opladen: Westdeutscher Verlag.

Kurz, Constanze/Rieger, Frank (2011): Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. Frankfurt: Fischer.

Lyon, David (2004): The Electronic Eye. The Rise of the Surveillance Society. Cambridge: Polity Press.

Lyon, David (2001): Surveillance Society. Monitoring Everyday Life. Buckingham: Open University Press.

Misoch, Sabina (2004): Identitäten im Internet. Selbstdarstellung auf privaten Homepages. Konstanz: UVK.

Perrot, Michelle (1987): Kulissen. In: Perrot, Michelle (Hg.): Geschichte des privaten Lebens. Von der Revolution zum Großen Krieg. Frankfurt: S. Fischer. S. 419-629.

Ranum, Orest (1986): Refugien der Intimität. In: Ariès, Philippe/Chartier, Roger (Hg.): Geschichte des privaten Lebens. Von der Renaissance zur Aufklärung. Frankfurt: S. Fischer.

Reichert, Ramón (2008): Amateure im Netz. Selbstmanagement und Wissenstechnik im Web 2.0. Bielefeld: transcript.

Roncière, Charles de La (1985): Gesellschaftliche Eliten an der Schwelle zur Renaissance. In: Duby, Georges (Hg.): Geschichte des privaten Lebens. Vom Feudalzeitalter zur Renaissance. Frankfurt: S. Fischer.

Rossiter, Clinton/Konvitz, Milton R. (1957: Aspects of Liberty. New York: Cornell University Press.

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

Samjatin, Jewgeij (1977): Wir. Zürich: Manesse Verlag.

Solove, Daniel J. (2008): Understanding Privacy. Cambridge: Harvard University Press.

Veyne, Paul (1989): Das Römische Reich. In: Veyne, Paul (Hg.): Geschichte des privaten Lebens. Vom Römischen Imperium zum Byzantinischen Reich. Frankfurt: S. Fischer.

Westin, Alan F. (1970): Privacy and Freedom. London: The Bodley Head.

Zeger, Hans G. (2008): Mensch. Nummer. Datensatz. Unsere Lust an totaler Kontrolle. St. Pölten: Residenz Verlag.

Onlinequellen

ARD-ZDF-Onlinestudie (2013a): Entwicklung der Onlinenutzung in Deutschland 1997 bis 2012. Online im Internet: http://bit.ly/OKSmke (Stand: 01.04.2013).

ARD-ZDF-Onlinestudie (2013b): Web 2.0: Gelegentliche und regelmäßige Nutzung 2007 bis 2012. Online im Internet: http://bit.ly/129bO3J (Stand: 01.04.2013).

ARD-ZDF-Onlinestudie (2013c): ARD/ZDF-Onlinestudie 2012. Online im Internet: http://bit.ly/MGBdwk (Stand: 01.04.2013).

BFDI (2012): Modernisierung des europäischen und nationalen Datenschutzrechts. Online im Internet: http://bit.ly/16cRanm (Stand: 25.02.2012).

Bütschi, Danielle/Hilty, Lorenz (2003): Das Vorsorgeprinzip in der Informationsgesellschaft: Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Online im Internet: http://bit.ly/13ZIMDG (Stand: 06.02.2011).

Cashmore, Peter (2009): Privacy is dead, and social media hold smoking gun. Online im Internet: http://bit.ly/4eotN3 (Stand: 11.09.2012).

Chaos Computer Club (2013): Hackerethics. Online im Internet: http://bit.ly/5uUgjH (Stand: 08.03.2013).

Civic Commons (2013): Open Data Policy. Online im Internet: http://bit.ly/mdZli5 (Stand: 31.01.2013).

Duden Online (2012): Privat. Online im Internet: http://bit.ly/WOPGqU (Stand: 29.03.2012).

Electronic Frontier Foundation (2012): Anti-Counterfeiting Trade Agreement. Online im Internet: http://bit.ly/9nEUVo (Stand: 04.04.2012).

Facebook (2013): Facebook's News Policy. Online im Internet: http://on.fb.me/WsFM1d (Stand: 08.02.2013).

Facebook Newsroom (2012): Key Facts. Online im Internet: http://bit.ly/SbkfpO (Stand: 14.12.2012).

Fasel (2011): Der Startschuss. Online im Internet: http://bit.ly/17IJA22 (Stand: 12.10.2012).

Geuter, Jürgen (2011): Privatsphärenkrücken. Online im Internet: http://bit.ly/10D3J2Y (Stand: 12.10.2012).

Geuter, Jürgen (2013): Rituelles Schattenboxen. Online im Internet: http://bit.ly/111G131 (Stand: 14.04.2013).

Google Flutrends (2013): Über Google Grippe-Trends. Online im Internet: http://bit.ly/Y9Jhgi (Stand: 29.03.2013).

Grossman, Lev (2006): Time's Person of the Year: You. Online im Internet: http://ti.me/vK5y (Stand: 06.01.2012).

Grundrechteschutz.de (2012): Recht auf informationelle Selbstbestimmung. Online im Internet: http://bit.ly/11P03xL (Stand: 04.12.2012).

Jander, Johannes (2001): Ugol's Law. Online im Internet: http://bit.ly/10f14N0 (Stand: 12.02.2013).

Koblin, John (2008): The Web Guru. Online im Internet: http://bit.ly/YqRH0m (Stand: 16.11.2012).

Lischka, Konrad (2011): Datenschutz-Kritik. Feinde der Freiheit. Online im Internet: http://bit.ly/17IJGXg (Stand: 27.03.2013).

McLuhan, Marshall (1974): Marshall McLuhan Speaks. End of Secrecy. Online im Internet: http://bit.ly/mJcQEF (Stand: 27.03.2012).

Mc Neally, Scott (1999): Sun on Privacy: Get Over It. Online im Internet: http://bit.ly/iX8Y (Stand: 26.03.2012).

Neumann, Linus (2011): Hidden Features in iOS4: Peilsender. Online im Internet: http://bit.ly/10D3Sn1 (Stand: 07.11.2012).

Pew Internet & American Life (2007): Teens, Privacy and Online Social Network. Online im Internet: http://bit.ly/13dK4fi (Stand: 18.02.2013).

Pew Internet & American Life (2010): The future of social relations. Online im Internet: http://bit.ly/bO1Mg9 (Stand: 18.02.2013).

Pew Internet & American Life (2012): Parents, Teens, and Online Privacy. Online im Internet: http://bit.ly/YBeNU9 (Stand: 18.02.2013).

Plomlompom (2011a): Informationelle Selbstbestimmung schafft Gedankenverbrechen. Online im Internet: http://bit.ly/oki3GY (Stand: 14.01.2013).

Plomlompom (2011b): Persönlichkeitsrecht = Persönlichkeitspflicht. Online im Internet: http://bit.ly/p3E52h (Stand: 14.01.2013).

Popcorn, Faith (2013): Super Cocooning. Online im Internet: http://bit.ly/13D2Dvh (Stand: 19.02.2013).

Post, Robert C. (2001): Three Concepts of Privacy. Online im Internet: http://bit.ly/17IJS8U (Stand: 15.12.2011).

Seeliger, Julia (2011): Jahreskongress des Chaos Computer Club. Der Innenminister als Troll. Online im Internet: http://bit.ly/tJ7yVw (Stand: 14.12.2011).

Seemann, Michael (2011): Datenschutz ist eine Brückentechnologie. Online im Internet: http://bit.ly/10f1enD (Stand: 06.02.2013).

Seeman, Michael (2011): Vom Kontrollverlust zur Filtersouveränität. Online im Internet: http://bit.ly/17IJV4N (Stand: 06.02.2013).

The Quantified Self (2013): Self knowledge through numbers. Online im Internet: http://bit.ly/cmERcJ (Stand: 08.07.2012).

Virtuelles Datenschutzbüro (2006): Informationelle Selbstbestimmung. Was bedeutet das? Online im Internet: http://bit.ly/107vZz2 (Stand: 24.01.2012).

Warren, Samuel D u. Brandeis, Louis D. (1890): The Right to Privacy. Online im Internet: http://bit.ly/11dghFM (Stand: 08.10.2012).

Interviews

Alvaro, Alexander (2011): Interview für Masterprojekt MIIO. Brüssel: Europäisches Parlament.

Beckedahl, Marcus (2011): Interview für Masterprojekt MIIO. Berlin: Chaos Communication Congress.

Hilty, Lorenz (2011): Interview für Masterprojekt MIIO. St. Gallen: EMPA.

Hustinx, Peter (2011): Interview für Masterprojekt MIIO. Brüssel: EDPS.

Kurz, Constanze (2011): Interview für Masterprojekt MIIO. Berlin: Humboldt Universität.

Sixtus, Mario (2011): Interview für Abschlussprojekt MIIO. Düsseldorf: Blinkenlichten Produktionen.

Zeger, Hans G. (2011): Interview. Wien: ARGE Daten.