Schriftenreihe
Forschungsforum Öffentliche Sicherheit

Technische Innovationen und deren gesellschaftliche Auswirkungen im Kontext von Überwachung

Nils Zurawski

Forschungsforum Öffentliche Sicherheit

Freie Universität Berlin

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Technische Innovationen und deren gesellschaftliche Auswirkungen im Kontext von Überwachung

Nils Zurawski

Forschungsforum Öffentliche Sicherheit

Herausgeber: Jochen Schiller, Lars Gerhold, Saskia Steiger, Gabriel Bartl, Helga Jäckel

Schriftenreihe Sicherheit Nr. 16, April 2015

Print: 978-3-944675-30-5 Online: 978-3-944675-31-2

Anschrift:	Tel: +49 (0)30 838 57367
Freie Universität Berlin	Fax: +49 (0)30 838 4 57367
Carl-Heinrich-Becker-Weg 6-10	www.schriftenreihe-sicherheit.de
12165 Berlin	kontakt@schriftenreihe-sicherheit.de

Autor:

Dr. Nils Zurawski habilitierte 2013 an der TU Darmstadt, Thema der Habilitationsschrift: Raum – Weltbild – Kontrolle. Überwachung und Vorstellungen von Gesellschaft als Faktoren sozialer Dynamik. Von April 2010 bis März 2013 Vertretungs/Gastprofessor am Fachbereich Sozialwissenschaften der Universität Hamburg, seit April 2013 war er Projektleiter des Teilprojektes IRiSS ebendort. Von Oktober 2013 bis April 2014 vertrat er die Professur für Kriminologie an der Universität Hamburg.

Kontakt zum Autor:

Universität Hamburg

Institut für kriminologische Sozialforschung

Allende-Platz 1

20146 Hamburg

Inhalt

1. Einleitung 7

1.1. Technische Innovationen und Anwendungsbereiche 7

1.2 Wissenschaft und Politik 9

2. Begriffsklärungen: Überwachung, Kontrolle, Datenschutz, Sicherheit und Macht 13

2.1. Überwachung 14

2.2. Kontrolle 15

2.3. Macht 17

2.4 Datenschutz/Privatsphäre 18

2.5 Sicherheit 20

2.6 Zusammenfassung: Begriffklärungen 22

3. Überwachung: Stand der Forschung und aktuelle Diskussionen 25

3.1.Theorie der Überwachung 26

3.1.1 Panopticon vs. assemblage/Netzwerk 26

3.1.2 Die flüchtige Moderne, Risiko- und Sicherheitsgesellschaft 29

3.1.3 Zusammenfassung: Theorie der Überwachung 32

3.2 Theorie in der Praxis von Überwachung 33

3.2.1 Big Data – Kategorien zur Kontrolle der Welt 34

3.2.2 Überwachung als social sorting 37

3.2.3 Überwachung und Technik 39

3.2.4 Überwachung als soziale Praxis und soziales Handeln 48

3.2.5 Überwachung als soziale Beziehung / Akteure der Überwachung 54

3.2.6 Zusammenfassung: Überwachung als Management gesellschaftlicher Probleme 56

4. Felder der Überwachung und technische Innovationen – Anwendungsfelder und Intentionen 59

4.1 Raum und Überwachung 60

4.2 Flughafen 65

4.3 Urbaner Raum und die smart cities 72

4.4 Zusammenfassung: Raum, Technik und angewandte Problemlösung 76

5. Technik und Überwachung – Konsequenzen und gesellschaftliche Wechselwirkungen 79

5.1 Kritik der Szenarien in der Sicherheitsforschung 80

5.2 Beispiele für Implikationen technischer Innovationen 86

5.2.1 Beispiel Flughafen 86

5.2.2 Beispiel Stadien und Mega-Events 91

5.2.3 Beispiel Bodycams 93

5.2.4 Beispiel vernetze Stadt und urbanes Management in der smart city 95

5.3 Zusammenfassung: Technik und Überwachung 98

6. Handlungsempfehlungen für die Sicherheitsforschung im Kontext von Überwachung 101

6.1 Politik 102

6.2 Wissenschaft 104

6.3 Unternehmen / zivile und staatliche Akteure 105

7. Literatur 107

1. Einleitung

In dieser Expertise wird der Frage nach den möglichen gesellschaftlichen Auswirkungen technischer Innovationen nachgegangen, die vor allem im weit gefassten Kontext von Überwachung eingesetzt werden oder eingesetzt werden sollen. Diese Aufgabe beschreibt ein enorm weites Feld, zu deren Bearbeitung ein paar Vorbemerkungen nötig sind. Zum einen um den Bereich der hier behandelten technischen Innovationen und ihrer Anwendungsgebiete einzugrenzen, zum anderen ein paar grundlegende Aspekte zum Spannungsfeld von Wissenschaft und Politik zu erläutern, die für die vorliegende Expertise wichtig sein werden, insbesondere als Vorgriff auf die Handlungsempfehlungen am Ende.

1.1. Technische Innovationen und Anwendungsbereiche

Aufgabe dieser Expertise ist es etwas über die Beziehung technischer Innovationen und ihrer gesellschaftlichen Auswirkungen auszusagen und zusammenzutragen. So gestellt, geht die Frage möglicher Konsequenzen von Sicherheitstechnologien auf Gesellschaft von der Prämisse aus, dass technische Innovationen allein durch ihre Existenz einen Einfluss haben und im Umkehrschluss, dass diese Innovationen, zumeist (digitale) Mess-, Regelungs-, oder Erfassungstechnologien, von oben auf Gesellschaft im weitesten Sinne herabfallen und dann Wellen schlagen wie ein Stein im Wasser. Beides ist nicht der Fall und zentral für diese Expertise. Technische Innovationen nur auf eine lineare Wirkung hin zu untersuchen, verkennt, dass Gesellschaft vielschichtiger ist, als eine solche Annahme voraussetzen würde. Wichtiger ist es stattdessen, die Wechselwirkungen von Technologien und Gesellschaft zu untersuchen, wobei sowohl gesellschaftliche Dynamik eine Rolle spielen darf, kontingentes Verhalten innerhalb von gesellschaftlichen Gruppen (Anwendern, Nutzern, Bürgern, Politikern, Technikern usw.), als auch die Technologie als materielle Kultur. Letzteres bedeutet im Kern, dass Technologien Dinge darstellen, die symbolisch und ideologisch aufgeladen sind, Bedeutungen transportieren und somit politisch und sozial nie neutral sind. Technologien, unter anderem verstanden als Anwendungen von Wissen und ausgestattet mit Materialität, einer Dinghaftigkeit, werden gemacht, mit ihnen wird umgegangen und sie sind Teil sozialer Beziehungen innerhalb von Gesellschaften, in denen ihnen Bedeutung zugeschrieben, diese verändert oder entzogen wird (vgl. Vannini 2009a). Gesellschaftliche Auswirkungen technischer Innovationen können nur adäquat ergründet werden, wenn technische Innovationen als Teil gesellschaftlicher Prozesse erkannt und entsprechend gerahmt werden. Die Vermutung, Technologien, z.B. Videokameras, die im öffentlichen Raum mit der Begründung der Verbrechensbekämpfung aufgestellt werden, würden einfach nur auf Gesellschaft einwirken, wird den Wechselwirkungen nicht gerecht, ebenso wenig wie die Annahme, dass man soziale

Probleme mit Technologien lösen könnte, oder nur die Logik einer Technologie auf Gesellschaft übertragen muss, um gewünschte Ergebnisse zu erzielen – z.B. Effizienzstrategien oder die Übertragung von Programmierideen von Computern auf Verhalten (vgl. Rieger 2015). Um am Ende dieser Expertise tatsächlich Handlungsempfehlungen geben zu können, die über den Rat „bitte den Datenschutz beachten" oder Designvorschläge hinausgehen, sollen hier die Felder der Anwendung technischer Innovationen vor dem Hintergrund erörtert werden, dass in ihnen (mit und ohne die Innovationen) gehandelt wird, und Technologien (insbesondere solche innerhalb des Feldes Sicherheit) daher keine neutralen Dinge sein, sondern Träger von Bedeutungen und Vermittler sozialer Beziehungen.

Das zentrale Anwendungsgebiet bzw. der Kontext, auf den sich diese Expertise bezieht, ist all jenes, was sich im weitesten Sinn mit dem Begriff Überwachung im Zusammenhang mit der Sicherheitsforschung verbinden lässt. Was ist genau damit gemeint? Ähnlich wie Sicherheit ist Überwachung ein Sammelbegriff, der mal ein Verfahren, mal eine Technologie, ein einzelnes technisches Artefakt, dann wieder eine Politik oder Weltanschauung beschreiben soll. Darunter könnte man von der Beobachtung des Wetters durch Weltraum-gestützte Satelliten bis hin zur Beschattung eines Verdächtigen durch die Polizei (oder einen Detektiv) so ziemlich alles verstehen, was nur im Entferntesten mit einer Form der Beobachtung zu tun hat. Und dabei bedeutet Überwachung nicht zwingend auch eine Kontrolle, so wenig wie Sicherheit und Überwachung zwei Phänomene sind, die auf der gleichen Ebene anzusiedeln sind. Sicherheitsforschung, zumal im Sinne des vom BMBF ausgelobten Programms gleichen Namens, hat ein gänzlich anderes Objekt und grundlegend unterschiedliche Zielsetzungen von der Überwachungsforschung (*surveillance studies*), wenn es letztere als solche denn so verstanden geben sollte.

Bevor also eine möglichst umfassende Aufarbeitung und Darstellung des aktuellen Diskussionsstandes zu dem Themenkomplex Überwachung, technische Innovationen, Sicherheitsforschung und gesellschaftliche Konsequenzen gemacht werden kann – und bevor darauf aufbauend bedeutende und virulente Fragestellungen herausarbeitet werden, müssen zunächst die Grundbegriffe geklärt werden. Das ist wichtig, um klar zu machen, wann innerhalb dieser Expertise von was die Rede ist und um die späteren Einordnungen und letztlich die Empfehlungen, offenen Fragen und deren zukünftige Relevanz zu verstehen.

Sicherheit und der Einsatz von Technik im Kontext von Überwachung ist auf keinen Fall linear zu denken. Die Details dieser Expertise vorwegnehmend kann gesagt werden, dass eine Technologie weder automatisch Sicherheit bringt, noch lässt sich jede Form der Überwachung skandalisieren. Und letztlich ist die Gesellschaft nicht beliebig steuerbar, auch wenn einzelne Erscheinungen von Gesellschaft zum Beispiel in bestimmten sozial-räumlichen Kontexten durch eine Steuerung (auch Überwachung

und Kontrolle) beeinflusst werden können. Wie bereits am Anfang deutlich gemacht, werden die mittelbar über Technologie zu erreichenden Ergebnisse oft verkürzt auf die Technologie selbst produziert – „Kameras verhindern Kriminalität“ – anstatt die Rolle von Technologie in diesem Zusammenhang zu reflektieren. Der Einsatz von Technologie geht häufig auf den Glauben an eine beliebig steuerbare Gesellschaft zurück, auf den Wunsch etwas zu tun, dieses Tun zu zeigen, öffentlich zu machen, was dann zu Formen symbolischer Politik führt. Letztlich berührt dieses Problem die Kommunikation zwischen Wissenschaft, insbesondere solcher, die sich kritisch und reflektiert mit Überwachung, Kontrolle und Sicherheit auseinander setzt, und der Politik bzw. den politischen Akteuren. Dazu gehört auch oft genug die Wirtschaft, die mit verkürzten Versprechen – Technik gegen den Terror, gegen Kriminalität, für Sicherheit – diese soziotechnischen Lösungen anbietet, dabei den wirtschaftlichen Erfolg ebenso sucht, wie man ihr eine Sorge um das Allgemeinwohl unterstellen kann. Das bedeutet, dass Sicherheit, insbesondere solche Konzepte, die mit Technologien als Lösungen arbeiten, im Spannungsfeld von Politik, gesellschaftlichem Wunsch und wirtschaftlicher Wertschöpfungskette steht. Eine nicht-technische, reflexive Wissenschaft, die sich mit den Widersprüchen solcher Konzepte befasst oder gar die gesellschaftlichen Konsequenzen jenseits der technischen Dimensionen beleuchten will, steht in einem problematischen Kommunikationsverhältnis zu den politischen Akteuren. Um die weiter unten aufgeführten Beispiele zu verstehen und einordnen zu können, wie welche Konsequenzen, Implikationen und Wechselwirkungen es konkret zwischen Technik, Überwachung, politischer Praxis sowie gesellschaftlicher Dynamik gibt, möchte ich hier ein paar Aspekte der Kommunikation von Wissenschaft und Politik beleuchten. Diese Aspekte sind auch wichtig um den Hintergrund und das Anliegen dieser Expertise besser einordnen zu können.

1.2 Wissenschaft und Politik

Politiker sind generell eher an Antworten denn an noch mehr und zusätzlichen Fragen interessiert. Wenn der Politiker nach einer Lösung für mehr Sicherheit in einem Bereich fragt, dann lauten die Antworten der Wissenschaft häufig: „Was für eine Sicherheit? Ist Sicherheit überhaupt der richtige Begriff? Geht es überhaupt um die Sache? Müssen wir uns nicht um andere Sachen kümmern?“ Oder es werden technische Lösungen präsentiert, die sich nur vermeintlich mit dem eigentlichen Problem befassen, die aber als Antwort auf eine Frage – z.B. Sicherheit an Flughäfen, Gewalt gegen Polizisten – verstanden werden. Es ist ein Dilemma, dass Demokratien auf einer zweifachen Legitimation beruhen: der Legitimation aufgrund der Delegation der Macht durch die demokratische Wahl und aufgrund der Rationalität politischer Entscheidungen durch den Bezug auf gesichertes und in der Wissenschaft möglichst konsistentes Wissen. Politik ist dabei nicht an von Wissenschaft (auch) vertretenen Ambivalenz interessiert.

Doch gerade diese lebt in vielen Disziplinen hingegen sehr gut mit Ambivalenzen. Werden politische Ambivalenzen von der Wissenschaft aufgezeigt, wird aus dem Kommunikationspartner ein Störenfried, dem zuzuhören lässlich erscheinen mag. Entscheidungen kann man letztlich auch ohne die Expertise der Wissenschaft fällen. Nun kann Wissenschaft Politik generell davon entlasten, Entscheidungen zu treffen eine solche Verlagerung der Entscheidungskompetenz würde auch demokratischen Grundsätzen widersprechen – Wissenschaftler sind ja nicht für eine solche Aufgabe gewählt worden. Die Aufgabe von Wissenschaft ist es jedoch entsprechendes Faktenwissen für eine sachlich fundierte Diskussion bereitzustellen. Gleichzeitig greift Politik auf Wissenschaft zurück – bisweilen als rational dekliniert, oft jedoch auch beliebig und gemäß einer parteipolitischen Linie. Die Frage ist dann aber wie gut diese Entscheidungen tatsächlich sind, wie nachhaltig und in wessen Interesse. Wenn aus Wissenschaft jedoch ausschließlich Politikberatung wird – in welchem Fall ihre Chancen gehört zu werden sich vergrößern würden – hat das auf die Arbeit und Ergebnisse von Wissenschaft sehr wahrscheinlich Einfluss und verändert sie substantiell. Die Aufgabe von (wissenschaftlichen) Kommissionen und ähnlichen Gremien ist es zunächst Wissen so aufzubereiten, dass es für Politikentscheidungen anwendbar ist sowie konsensfähige Entscheidungsgrundlagen für die Politik erarbeitet werden. Das aber entbindet auch Wissenschaft nicht von der Verantwortung für die Folgen von Beratung und ihren Konsequenzen. Politikberatung ist auf einen diskursiven Prozess der Wissenserfassung und der Wissensbewertung angewiesen (Evers/Novotny 1987). Daraus ergibt sich zumindest ein stetes Spannungsverhältnis, welches in der Interaktion jedes Mal neu ausgehandelt werden muss.

Wissenschaft, die im Dienst der Politik steht, kann nicht länger eigenständiger Impulsgeber sein, im Sinne einer freien, unbestimmten Forschung, die schaut, welche Probleme sich aus der Betrachtung von Gesellschaft und Politik ergeben. Es mag hier eingeworfen werden, dass Forschung, die wie in Deutschland weitgehend staatlich alimentiert ist, tatsächlich frei ist, aber das würde hier doch zu weit führen. Somit sind es oftmals falsche Voraussetzungen, unter denen sich Politik und Wissenschaft treffen. Es zeigt sich dabei, dass beide unterschiedliche Vorstellungen von der Wirklichkeit haben, z.B. bezogen auf das Thema Sicherheit oder so genannte Bedrohungslagen. Die jeweiligen Antworten darauf hängen dann von solchen Vorstellungen ab und fallen entsprechend unterschiedlich aus. Hier besteht so etwas wie eine Kommunikations-barriere, die sich durch Wahrnehmungsdifferenzen, bezogen auf die Ziele und jeweiligen Rationalitäten und Handlungsrahmen der Akteure, erklärt. So interessiert sich die Politik besonders in der Sicherheitsforschung an dem, was in Zukunft sein könnte. Indem auf solche Möglichkeiten Antworten gesucht und gefunden werden, werden materielle Fakten geschaffen, die dann eine eigene Wirklichkeit einnehmen. Das gilt insbesondere für in diesem Zusammenhang entstandene technische Innovationen. Wissenschaft auf der einen Seite will Aufklärung und Diskurs und nutzt Wirklichkeit

als Folie der Erkenntnis und als Material der Empirie, um daraus unter Umständen Aussagen über die Zukunft zu treffen. Politik hingegen will die Wirklichkeit formen.

Diese Bemerkungen sollen vorausgeschickt werden, um zum Einen auf mögliche Verständnisprobleme beim Lesen dieser Expertise hinzuweisen, die sich eben genau aus den unterschiedlichen Zielen und Erwartungen verschiedener Akteure ergeben. Zum Anderen wird damit das Gebiet der Expertise – technische Innovationen, Überwachung und gesellschaftliche Auswirkungen – abgesteckt. Denn gerade im Bereich von Sicherheit kommen diese Aspekte zusammen und werden als Teil einer rahmenden Symbolik oft mit Bedeutungen aufgeladen, deren Grad und Wirkung hier heraus gearbeitet werden soll. Kommunikation zwischen Akteuren ist dabei, das wird noch zu zeigen sein, ein wichtiges Element.

Diese Expertise bietet eine wissenschaftliche, zumeist soziologische Erörterung von Überwachung im Hinblick auf Sicherheit und Technologie – verstanden als Diskussionsgrundlage mit den Akteuren aus Politik, Staat, Industrie und Zivilgesellschaft.

2. Begriffsklärungen: Überwachung, Kontrolle, Datenschutz, Sicherheit und Macht

In vielen populären Debatten und Beiträgen werden die Begriffe Überwachung und Kontrolle synonym verwendet. Wenn von Überwachung die Rede ist, wird sehr häufig ein Datenschützer befragt, nach den Snowden-Enthüllungen wurde nach einem verbesserten Datenschutz und entsprechenden Gesetzen verlangt, obwohl deren Mangel nicht das eigentliche Problem gewesen ist, sondern im Gegenteil, diese Gesetze einfach missachtet wurden. Datenschutz ist demnach nicht das logische Partnerargument zu Überwachung oder Kontrolle. Im Kontext von Sicherheit, insbesondere öffentlicher, ziviler Sicherheit ist auch von Überwachung die Rede, doch anders als mitunter suggeriert wird, wäre eine Sicherheitsgesellschaft nicht nur ein anderer Begriff für eine Überwachungsgesellschaft, Überwachung nicht die logische Folge von einem Primat der Sicherheit und schon gar nicht ihr Synonym. Wie also unterscheiden sich die einzelnen Begriffe und die Phänomene, die damit verbunden sind? Und was beschreiben die jeweiligen Begriffe für sich? Eine Aufarbeitung der Zusammenhänge von technischen Innovationen im Hinblick auf ihre Bedeutung für mögliche gesellschaftliche Auswirkungen (bzw. die vielfältigen Wechselwirkungen zwischen ihnen), braucht zunächst analytisch trennscharfe Definitionen – auch wenn diese in der Praxis nicht immer so durchgehalten werden kann.

Grundsätzlich lässt sich für eine Unterscheidung schon jetzt festhalten:

- **Überwachung** und **Kontrolle** beschreiben Verfahren, sind Tätigkeiten, die sich in Praktiken entwickeln, die zum Teil durch Technologien vermittelt ausgeübt werden, bzw. die sich in der Ausübung einer Praktik als solche manifestieren. Letzteres bedeutet, dass nicht alles, was in der wissenschaftlichen Analyse als Überwachung oder Kontrolle genannt wird, in der Praxis als solche bezeichnet oder als solche erkennbar ist.

- **Sicherheit** ist demgegenüber ein Zustand, der erreicht wird oder werden soll, gestört oder gefährdet wird und Ziel oder Mittel (von Politik, Technik, Gesellschaft) sein kann. Überwachung und Kontrolle sind Verfahren, die zur Erreichung dieses Zustandes eingesetzt werden. Das Risiko ist in diesem Zusammenhang eine Form der Operationalisierung, mit der der Grad des Zustandes Sicherheit bestimmt bzw. zukünftige Handlungen rationalisiert werden können. Hier geht es im Wesentlichen um sozial bewertete Wahrscheinlichkeiten.

- **Datenschutz** beschreibt zunächst nichts anderes als ein Rechtsgebiet, mit dem der Fluss von Informationen geregelt wird. Die grundlegenden Prämissen sind normativ sowie ethisch-moralisch festgelegt. **Privatsphäre**, als diskursives Element eng mit dem Datenschutz verbunden, ist nicht mit diesem gleichzusetzen, sondern beschreibt

ein Rechtsgut und somit eine soziale Größe, die mal ethisch, mal rechtlich bewertet werden kann.

- Der Begriff der **Macht** kommt in diesen Analysen oft vor und ist ein zentrales Phänomen, wie in den Ausführungen zu erkennen sein wird. Macht ist eine soziologische Größe, die der Analyse und Beschreibung dient und somit auf einer anderen Ebene anzusiedeln ist. Sie ist weder eine Tätigkeit, noch ein Rechtsgut oder ein Zustand.

2.1. Überwachung

Ungeachtet der bereits angedeuteten breiten Verwendung des Begriffes Überwachung – von der Beobachtung anderer bis hin zu einem Monitoring des Weltklimas durch Satelliten– kann sie ganz generell als ein ***Phänomen der Schaffung, Steuerung und Erhaltung gesellschaftlicher Ordnung*** definiert werden (vgl. Lyon 2002). Überwachung ist in diesem Sinne eine Orientierungsleistung von Akteuren, mit der diese sich einen Überblick über die Welt oder geographische, politische, soziale Ausschnitte davon verschaffen. Typisch für Überwachung ist dabei ein tendenziell asymmetrisches Verhältnis zwischen den Akteuren (Überwacher-Überwachte) und eine darauf aufbauende, hierarchische Kontrolle und Steuerung von Gesellschaft (vgl. Zurawski 2014). Die Bedeutung von Informationen und deren Klassifizierung und Kategorisierung ist zentral für Überwachung. Überwachung zielt darauf ab, vorgegebene Normen mit technischen oder nicht-technischen Monitoring-Systemen zu überprüfen. So gesehen soll Überwachung nicht nur ein modisches Synonym für soziale Kontrolle sein. Es handelt sich nicht um eine soziale Kontrolle mit technischen (heute: digitalen) Mitteln. Wie und wo sich Überwachung manifestiert und ob eine Technologie dabei immer die zentrale Rolle spielt, oder nicht auch nur ein Medium sein kann, im Sinne der Ermöglichung einer Kontrolle oder Steuerung von Menschen oder Prozessen, ist mit dieser Definition nicht erklärt.

Überwachung ist gegenwärtig vor allem vor dem Hintergrund einer fast vollständigen Informatisierung von Gesellschaft zu sehen, welche unter dem Stichwort Informationsgesellschaft bereits Eingang in den Alltag und populäre Diskurse gefunden hat. Dennoch ist dieser Rahmen noch kein zwingender Grund, eine Kamera synonym mit Überwachung zu setzen oder bei jeder Datenbank gleich an Rasterfahndung zu denken. Gegenwärtige Diskussionen über Datenschutz, Biometrie, Kriminalität und Terrorabwehr legen eine solche Vermutung nahe (und sind teilweise gerechtfertigt). Die Informatisierung allein allerdings gleichzusetzen mit Überwachung, würde bedeuteten, nur auf die Symptome zu schauen ohne ein Verständnis dafür, welche Besonderheiten hinter einer Technik oder gesellschaftlichen Praxis stehen, über die sich Überwachung konstituiert und diese im Besonderen ausmacht – und wie es darüber in die

gesellschaftliche Dynamik eingreift oder diese in einigen Bereichen überhaupt erst möglich macht. Die Überwachungsgesellschaft ist ein Teil der Informations-gesellschaft, aber beide sind auf keinen Fall deckungsgleich. Zusammenfassend soll festgehalten werden, dass Überwachung eine Ansammlung von Praktiken darstellt und im Zusammenhang mit Machtverhältnissen zu sehen ist, welche die Beobachter privilegieren.

Überwachung ist angelegt auf die Sammlung und Verarbeitung von Daten gleich welcher Art (diese müssen nicht notwendigerweise digital sein). Dazu werden Kategorien und Klassifikationen geschaffen, nach denen eine Überwachung stattfinden kann, an der sie sich orientieren kann – darin ähnelt sie sozialer Kontrolle. Das bedeutet auch, dass es sich nicht zwingend um soziale oder rechtliche Normen handeln muss, die überwacht werden, sondern Überwachung auch losgelöst von diesen stattfinden kann. So spiegelt sie Machtverhältnisse und Strukturen wider, die nicht notwendigerweise sozial akzeptiert sind Je bürokratisierter jedoch die Formen der Überwachung und je zentraler die Instanzen ihres Ursprungs werden, desto deutlicher können sich Überwachung und soziale Kontrolle unterscheiden. Mit Bauman, der Überwachung von dem Zweck bestimmt sieht **Ziele auszumachen, zu orten, im Blick zu behalten** (Bauman & Lyon 2013, 116), würde eine Unterscheidung zu sozialer Kontrolle durch Bestimmtheit, mögliche Vorausschau und die strategische Planung (*im Blick behalten*) gekennzeichnet sein. Dabei würden auch Informationen gesammelt.

2.2. Kontrolle

Kontrolle in nur wenigen Worten von Überwachung zu unterscheiden ist nicht einfach. Unstrittig ist, dass beide Phänomene miteinander verzahnt sind und im Alltagsgebrauch der Begriffe oft synonym benutzt werden. Dennoch lassen sich einige wichtige Unterschiede finden, die auch im Hinblick auf eine Bewertung technologischer Innovationen wichtig werden können.

Rule (1974) grenzt Überwachung von einer sozialen Kontrolle dahingehend ab, dass Überwachung primär mit dem Sammeln und Auswerten von Informationen zu tun hat, in diesem Sinne zielgerichtet ist. Systeme der Kontrolle bezeichnet er hingegen als notwendig, um Sanktionen zu verhängen und durchzusetzen. Ich möchte mich dieser minimalen, aber weitreichenden Unterscheidung anschließen.

Überwachung als das routinemäßige Sammeln und Auswerten von Daten erfordert nicht zwingend die Existenz einer Form übergeordneter und systematischer (sozialer) Kontrolle. Und (soziale) Kontrolle bedeutet nicht zwangsläufig eine systematische Überwachung, die sich auf ein Objekt konzentriert und dieses – geleitet durch externe Kategorien und Klassifizierungen – bewertet und entsprechende Handlungen auslöst.

Das Konzept von sozialer Kontrolle spielt vor allem in Verbindung mit abweichendem Verhalten eine zentrale Rolle. Abweichendes Verhalten darf dabei nicht nur in einem kriminologisch-strafrechtlichen Sinn verstanden werden, sondern muss sich auf Normverletzungen im Allgemeinen beziehen. Soziale Kontrolle ist ein immanenter Teil von Gesellschaft. Im positiven Sinn als Teil der sozialen Integration oder bei Normenverletzungen zur Disziplinierung des Einzelnen (vgl. Stolle & Singelnstein 2008: 95ff). Scheerer schlägt vor, soziale Kontrolle als das *„Ensemble all dessen zu definieren, was unerwünschtes Verhalten verhindern soll und/oder faktisch verhindert"* – wobei auch der Versuch der Verhinderung ein Kontrollverhalten sein kann. Ebenso soll alles, was auf unerwünschtes Verhalten reagiert, als soziale Kontrolle definiert sein (Scheerer 2000: 167).

Überwachung als soziale Kontrolle bedeutet dann, einen bestimmten Ausschnitt sozialen Lebens zu benennen, in dem Überwachung stattfindet. Überwachung kann so zu einem immanenten Bestandteil sozialer Kontrolle werden, ist aber nicht zwingend diese selbst. Kontrollen auf allen Ebenen – im sozialen Nahbereich, an kontrollierten Übergängen (Grenzen, Eingängen etc.) – oder in punktuellen Überprüfungskontexten beruhen oftmals auf der vorhergehenden Überwachung von Verhalten bzw. der Sammlung von Informationen, die dann mit einem Verhalten, einer Situation oder einer konkreten Person abgeglichen – kontrolliert – werden. James Rule (1974) hat daher bereits in seiner Analyse zur Informationsgesellschaft unter Überwachung das Sammeln und Aufbewahren von Informationen verstanden und Kontrolle als das beschrieben, was Organisationen oder Personen tun, um die Kontrolle über eine Situation zu behalten, insbesondere in Bezug auf das Management von Verhalten durch Sanktionen oder Ausschluss. Kontrollen sind demnach als Maßnahmen der Überprüfung mit dem Ziel des Durchgangs oder des Ausschlusses definiert. Wenn man dieses Verständnis zugrunde legt, dann ist das Sammeln von Daten im Internet durch Behörden oder Unternehmen eine Überwachung, aber noch nicht zwingend eine Kontrolle. Videoüberwachung im öffentlichen Raum würde beide Bereiche betreffen, wobei der Raum und nicht primär die Menschen als Individuen überwacht würden, wohl aber deren Verhalten kontrolliert werden soll – wobei diese Kontrolle auf der Annahme basiert, dass die Existenz der Kamera zu einer Art von Selbstkontrolle führt, die die Menschen abweichendes Verhalten von allein einstellen lässt (vgl. zu einer detaillierten Diskussion der Videoüberwachung dazu Zurawski 2009, 2014). Die Überprüfung von Personen, z.B. an Grenzen zur Identitätsfeststellung ist Kontrolle. Der PIN-Code einer Bankkarte, eine Unterschrift oder auch biometrische Merkmale wären dann Kontrollinstrumente, die zunächst nicht auf einer Überwachung basieren, sondern punktuell abgerufen werden, um an einem speziellen Punkt eine Überprüfung vorzunehmen. In vielen Fällen allerdings werden dazu Informationssammlungen benötigt, an denen dann der Abgleich stattfinden kann.

Auch wenn sich Beispiele finden lassen, wo solche Unterscheidungen in der Praxis aufgeweicht werden, soll Kontrolle zunächst auf die Überprüfungen festgelegt werden, denen nicht notwendigerweise eine dauerhafte Überwachung zugrunde liegen muss.

2.3. Macht

An dieser Stelle soll auch noch einmal auf den Begriff der Macht Bezug genommen werden, da er im Zusammenhang mit Überwachung und Kontrolle eine zentrale Rolle spielt. Macht, so die Definition von Max Weber (vgl. 1972, 28), bedeutet jede Chance, innerhalb eine sozialen Beziehung den eigenen Willen auch gegen Widerstände durchzusetzen, gleichwohl worauf diese Chance beruht. Diese zwar minimale, doch sehr grundsätzliche Definition von Macht kann ergänzt werden von den Gedanken Foucaults, der sich mit einer Analytik der Macht beschäftigte, aber eben keine grundlegende Theorie formulieren wollte (vgl. Lemke 2005, 319ff). Er hat die Machttechniken als Diskurse im historischen Kontext erforscht, in denen Wissen, die Produktion der Diskurse sowie die Prozesse der Regulierung zentrale Bedeutung haben. Damit ist kein Gegensatz zu Weber formuliert, sondern es handelt sich um eine gänzlich andere Herangehensweise. Eine weitere Definition von Popitz untersucht vor allem die Phänomene der Macht, also wie es im Anschluss an Weber dazu kommen kann, dass man den eigenen Willen gegen Widerstände durchsetzen kann. Dabei ist außer der Gewalt (im Sinne physischer, verletzender Gewalt), dem wohl stärksten Mittel in unserem Zusammenhang, vor allem die von ihm als *datensetzende Macht* bezeichnete Macht interessant (vgl. Popitz 1992, 29f). Weitergehend als Weber zeigt Popitz die verschiedenen Möglichkeiten von Macht auf und definiert diese. Eine datensetzende Macht kann man u.a. in Statistiken wiederfinden, in gesetzten Normen, oder in Klassifikationen auf Basis von gesammelten Daten, womit diese Definition der Machtausübung für die Betrachtung von Überwachung und Kontrolle interessant und fruchtbar ist. Ob und wie die Überschneidungen der einzelnen Ansätze aussehen, soll hier nicht weiter thematisiert werden. Wichtig allein ist, dass Macht Teil von Kontrolle und Überwachung sein kann. Zwar muss sie das nicht immer sein, ist aber (wenn vorhanden) als Grundlage für die Prozesse anzusehen. Überwachung kann somit der Ausdruck von Machtverhältnissen sein, die sich in der Möglichkeit zeigen, eine Technik, ein Verfahren anzuwenden und als verpflichtend auszugeben, z.B. beim Alkoholtest bei einer polizeilichen Verkehrskontrolle. Ebenso kann eben diese Möglichkeit in einer Technologie Anwendung finden, nämlich dann, wenn man sich einem dort vorgesehenen Zwang (oder der Verführung) nicht entziehen kann und die Macht somit vermittelt darüber ausgeübt wird, wie z.B. eine Identitätsabfrage per PIN-Code am Geldautomaten. Eine anonyme Geldabhebung ist nicht möglich. Wichtig ist dabei, dass Macht nicht skandalisiert werden darf, sondern zunächst nur die Verhältnisse sozialer Beziehungen kennzeichnet, deren Auswirkungen dann einer Bewertung

zugeführt werden können. Eine Bewertung der Machtverhältnisse kann erst im Anschluss vorgenommen werden und ist dann gleichzeitig eine Bewertung sozialer Verhältnisse bzw. der Bedeutung technischer Innovationen, über die möglicherweise asymmetrische soziale Verhältnisse begründet oder weitere Partizipationsmöglichkeiten verhindert werden.

2.4 Datenschutz/Privatsphäre

In dem Überwachungsdiskurs wird Datenschutz sehr häufig in einem Atemzug mit Überwachung genannt. Das ist jedoch zu kurz gegriffen und hat zu einer Skandalisierung des Begriffes Daten geführt, hinter dem fast immer eine Verletzung des Datenschutzes, der Privatsphäre, oder des Missbrauches von persönlichen Informationen vermutet wird. Daten oder Informationen sind ein elementarer Teil moderner, auf Bürokratie fußender Gesellschaften. Der Umgang des Staates mit den Informationen seiner Bürger ist der Ursprung des modernen Datenschutzrechtes, da informationelle Verhältnisse auch immer Machtverhältnisse darstellen können (vgl. von Lewinski 2012). Die Geschichte ist reich an Beispielen, wo Informationen zum Schaden Einzelner oder ganzer Bevölkerungsgruppen missbraucht wurden. Datenschutz und die Gesetze des Datenschutzes regeln diese informationellen Verhältnisse in einer als Informationsgesellschaft bezeichneten Moderne (vgl. Rule 1974; Lyon 1988; Castells 1996), die durch die Computer und Kommunikationstechnologien gekennzeichnet ist und dabei insbesondere die Verarbeitung von Informationen (Daten) in den Mittelpunkt gesellschaftlicher Dynamik rückt. Giddens verweist darauf, dass Informationen über Bürger und eine daran hängende Bürokratie (vgl. ebd. 1984, 180) zu den konstitutionellen Elementen moderner Staaten gehören und somit der moderne Staat auch durch Strukturen der Überwachung und Kontrolle geprägt ist, die auf Informationen beruhen. Ein Datenschutz jeglicher Ausprägung setzt an diesem Umstand an.

Geschützt werden soll durch die entsprechenden Gesetze auch die so genannte Privatsphäre, eine nicht absolute, kulturell unterschiedlich verhandelte und bestimmte Größe. Auch hier geht es letztendlich um eine Bestimmung von informationellen Verhältnissen, die die Berechtigungen und Eingriffsrechte in die Informationsflüsse zwischen Menschen, Gruppen von Menschen sowie zwischen Menschen dem Staat und auch Unternehmen regelt. Dabei ist die Privatsphäre nicht das Gegenstück zu Überwachung, sondern ein rechtlich-moralisch-soziales Phänomen, deren Integrität der Datenschutz u.a. garantieren soll, mit oftmals weitreichenden Ausnahmen, auch weil Privatsphäre durchaus als Objekt von Interessenskonflikten behandelt werden kann – Schutz individueller Interessen gegenüber dem Gemeinwohl oder wirtschaftlichen Bestrebungen (vgl. u.a. Rule & Greenleaf 2008, Lewinski 2012; zur Geschichte des Datenschutzes in Deutschland auch Hannah 2010; ein aktueller Überblick Schmidt &

Weichert 2012). Die Privatsphäre ist ein individualistisches Konzept, so wie der Datenschutz generell auf den Schutz privater Daten, d.h. individueller Daten ausgerichtet ist. Dieses Konzept ist, wie u.a. Nissenbaum und Coll (vgl. Nissenbaum 2004; Friedman et al. 2006; Coll 2011, 2012, 2014, Bennett 2011, Stalder 2002) aufführen, überdenkenswert, weil es im Hinblick auf Überwachung des informationellen Flusses zwischen einzelnen Personen auch hinderlich sein kann, oder wie Coll (2014) ausführt zu einem Verbündeten der Überwachung selbst werden kann.

Nissenbaum schlägt als Erweiterung eines nur auf das Individuum zugeschnittenen Konzeptes der Privatsphäre (*privacy*) den Ansatz einer *contextual integrity* vor, in der die Kontexte des Informationsflusses berücksichtigt werden. Ihr geht es dabei vor allem darum, den angemessenen Schutz von Informationsflüssen zwischen Personen oder Personen und Institutionen (staatlich und privat) im jeweiligen Kontext zu regeln – letztlich um die Informationen über eine Person besser schützen zu können. Das Argument, jemand würde ja auf Facebook auch etwas posten, deswegen sei es für alle anderen Zwecke frei verwendbar und nicht geschützt (z.B. Polizeiarbeit, andere Unternehmen usw.), würde nach dem Konzept der *contextual integrity* nicht zulässig sein, weil die Informationen in einem andern Kontext geäußert worden sind, andere Verwendungen also ihre Integrität verletzen würden. Familieninterna sind ja auch keine Geheimnisse und oftmals einem größeren Familienkreis bekannt, deshalb aber nicht von diesen an andere, nicht Eingeschlossene weiterzugeben. So kann man auch Informationen in sozialen Netzwerken (hier gemeint: *social media*) verstehen und entsprechend behandeln. Auch Coll betrachtet Privatsphäre nicht als etwas Absolutes, sondern als ausgehandelte, variable Größe, die u.a. Informationsflüsse regelt und den angemessenen Umgang mit Informationen über eine oder mehrere Personen in spezifischen Kontexten regelt. Er kritisiert im Zusammenhang mit Überwachung, dass die gesetzliche Definition von Privatsphäre den Kontext weitestgehend ausblendet, und so einer Überwachung bzw. einer Kontrolle im Sinne eines Managements von Individuen mehr hilft, als dass sie die Informationsflüsse beschützt. Wenn das Private absolut und vor allem vordefiniert festgelegt ist, dann engt das die Spielräume von Personen ein. Freiheiten sind nur innerhalb gesetzter Grenzen möglich, innerhalb von Grenzen, die festlegen, was privat ist und was nicht. Coll bezeichnet deshalb auch das bestehende Konzept von Privatsphäre als Verbündeten der Überwachung (2014, 4 *partners-in-crime*).

So verstanden ist Datenschutz eine wichtige Größe in der Debatte über Überwachung und Kontrolle, aber weder eine zwingende Größe zu jedweder Beurteilung einer Technologie oder Maßnahme, noch der zentrale Schlüssel zum Verständnis von

Überwachung, ihrer Konstituierung oder gesellschaftlichen Bewertung[1]. Eine Skandalisierung des Gebrauches von „Daten“ und Informationen über eine Person hilft einer solchen Analyse nicht. Das Verständnis dafür, dass gegenwärtige Überwachung eng an die Merkmale einer Informationsgesellschaft gebunden sind, hilft allerdings dabei, die Dimensionen von Überwachung, wie sie sich in der Regel heute darstellt und wahrgenommen werden kann, besser zu verstehen. Der Datenschutz ist dabei der rechtliche Rahmen, durchaus veränderbar, jedoch weder die Lösung, noch die analytische Blaupause zur Bewertung.

Überwachung und Privatsphäre sind zwei voneinander unabhängige Größen, zwischen denen der Datenschutz vermitteln kann.

2.5 Sicherheit

Sicherheit ist ein Zustand. Allerdings kann der Begriff auf so viele Bereiche bezogen werden und so unterschiedliche Bedeutungen annehmen, dass eine einheitliche Definition nicht nur unmöglich, sondern unsinnig erscheint. In dieser Expertise soll es um das begriffliche Verständnis von Sicherheit gehen, wie es im Sicherheitsforschungsprogramm der Bundesregierung wiedergegeben wird. Im Mittelpunkt stehen dabei Lösungen, die den Schutz der Bevölkerung und der kritischen Infrastrukturen vor Bedrohungen durch Terrorismus, Sabotage, organisierter Kriminalität, Piraterie, aber auch vor den Folgen von Naturkatastrophen und Großunfällen gewährleisten und so unseren freiheitlichen Lebensstil schützen.[2] Das bedeutet, dass es um die Art von Sicherheit geht, die von so genannten Sicherheitskräften wie den Behörden und Organisationen mit Sicherheitsaufgaben (BOS) hergestellt und somit auch im weitesten Sinne definiert wird (in diesem Sinn: *Sicherheit ist, was der Staat als solche definiert*). Der normative Charakter des Begriffes findet hier eine Erklärung. Jenseits einer normativen Bestimmung von ziviler Sicherheit, geht es analytisch um die Verwundbarkeit des modernen Lebens, welches nicht nur von technischen Unsicherheiten bedroht scheint – Atomkraftwerke, technische Unfälle, Störung von Infrastrukturen etc. – sondern auch von den strukturellen Unsicherheiten moderner Gesellschaften im Hinblick auf Arbeit, soziale Absicherung, Altersarmut, Gesundheit u.a. (vgl. Haverkamp et al. 2011, S. 9f; kritisch auch Beck 1986). Die Annahme, dass der Unfall die traurige Ausnahme der Moderne ist und nicht eines ihrer strukturellen Begleiterscheinungen, wie es der französische Philosoph Paul Virilio beschreibt (vgl. Virilio 2009, auch Breuer 1992) ist problematisch, wenn es um die Bewahrung des

[1] Vgl. Möllers/Hälterlein 2013: 57: In dealing with surveillance, scholars have widely agreed to refute privacy as an analytical concept and defining theme [...] because it is regarded as too narrow to grasp the entirety of the social consequences resulting from surveillance practices“,

[2] http://www.bmbf.de/pub/Rahmenprogramm_Sicherheitsforschung_2012.pdf S.2

Zustandes geht. Das Versprechen auf Sicherheit wächst mit den Risiken, kann aber nie zu deren Ausschluss führen, sondern, so Beck, muss immer wieder notdürftig und mit kosmetischen Eingriffen bekräftigt werden (vgl. ebd. 1986, 26).

Weniger geht es hier um die sogenannte Produkt- oder Umgangssicherheit (*engl. safety*), die in diesen Fällen nur am Rande eine Rolle spielen kann, nämlich dann, wenn von öffentlicher Sicherheit die Rede ist, die nicht unbedingt auf eine Produktsicherheit zu reduzieren ist, aber eben auch keine Sicherheit im oben genannten Sinn meint. Zu nennen wäre hier beispielhaft das britische Konzept der *community safety*[3], welches auf die Integrität einer Gemeinschaft verweist. Ebenso ist der Begriff des subjektiven Sicherheitsgefühls nicht zwingend an Terror, Kriminalität oder andere tatsächliche Gefährdungslagen gebunden, auch wenn dieses oft als gegeben vorausgesetzt scheint (vgl. Zurawski 2007; Schewe 2009, 93-131).

Sicherheit ist also ein Zustand, den es zu erreichen oder zu bewahren gilt. Überwachung und Kontrolle als Verfahren spielen dabei eine wichtige Rolle, z.B. indem Personen überwacht werden, denen man eine Störung dieser Sicherheit zutraut, oder indem Bereiche mit Kontrollstellen ausgestattet werden, an denen eine Störung der zivilen Sicherheit für möglich gehalten wird. Sicherheit und Überwachung/Kontrolle sind auf keinen Fall gleichzusetzen. Allerdings herrscht eine begriffliche Unklarheit, wenn Sicherheitstechnologien vor allem auf die Überwachung bzw. die Kontrolle von Individuen oder ganzer Bevölkerungsgruppen abzielen. Sicherheitstechnologien beschreiben Technologien, mit denen der Zustand der Sicherheit gewährleistet oder mit denen Gefährdungen dieses Zustandes antizipiert werden sollen. Das Risiko ist die Größe mit denen solche vorausschauenden Handlungsstrategien operieren (vgl. u.a. Beck 1986; Münkler et al. 2011; Haverkamp et al. 2011).

Kritisch zu sehen an den Konzepten der Sicherheit ist vor allem ihr normativer Charakter, der nicht berücksichtigt, dass der Zustand der Sicherheit gesellschaftlich konstruiert ist – also durchaus auch politischen, gesellschaftlichen oder wirtschaftlichen Interessen unterliegen kann und daher nicht absolut zu sehen ist (vgl. Monahan 2010; Bonß 2011). Und es gilt zu berücksichtigen, dass das Konzept von Sicherheit eng an die Idee eines Ausschlusses von Gefahren, u.a. über eine Risikobewertung, gebunden ist. Diese Perspektive auf mögliche, zukünftige gesellschaftliche Probleme, d.h. ihre Klassifizierung als Sicherheitsproblem, wird auch mit dem Begriff der Versicherheitlichung verbunden, in dem die konstruktive Qualität des erwünschten Zustandes Sicherheit über ein Problem klar zu Tage tritt (Bigo et al. 2010; Daase 2013; Masala & Fischer 2015). Eine Versicherheitlichung eines Problems, also die strukturelle Fassung eines nahezu beliebigen gesellschaftlichen Phänomens als sicherheitsrelevant – z.B. Migration, Aufnahme von Flüchtlingen, Kleinkriminalität, Umwelt usw. – definiert die

[3] http://www.communitysafety.qld.gov.au/ (5.1.2015)

Auswahl der Mittel und setzt rhetorische Grenzen des Umganges mit einem solchen Phänomen. Sicherheit als rhetorisches Mittel zur Definition eines Zustandes bzw. des Risikos seiner Verletzung impliziert oftmals eine Überwachung und hilft als Argumentation bei der Durchsetzung von Überwachungs- und Kontrollmaßnahmen. Hierin liegt die Verbindung der beiden Begriffe.

Sicherheit steht somit im Spannungsverhältnis zwischen normativem Begriff – Technologien der Sicherheit, technische Innovationen im Bereich öffentliche und zivile Sicherheit – und zu analysierender Größe. **Sicherheit (und Unsicherheit) ist ein Konstrukt von Politik und gesellschaftlicher Dynamik,** wobei hier nicht von unidirektionalen Kausalität auszugehen ist, sondern sich die Möglichkeiten für Konstruktionen und die erstellten Konzepte gegenseitig bedingen. Diese Spannung ist zentral für spätere Bewertungen und Handlungsempfehlungen in Bezug auf die Bedeutung und Auswirkung technischer Innovationen auf Gesellschaft.

2.6 Zusammenfassung: Begriffklärungen

Überwachung und **Kontrolle** sind sich ergänzende Ensembles von Handlungen, die zur Herstellung einer normativ konstruierten **Sicherheit** eingesetzt werden können. Grundlage dafür sind darin eingeschriebene **Machtverhältnisse**. Diese müssen nicht zwingend zwischen Staat und Bürgern bestehen, sondern können vielfältige, jeweils reziproke Konstellationen betreffen – Bürger-Bürger, Staat-Bürger, Unternehmen-Bürger (vgl. Bennett 2008 für eine Klassifizierung dieser Konstellationen, auch Zurawski 2014). Die Macht kann dabei offen durch Zwang sicht- und spürbar werden oder verdeckt und subtil in so genannten Macht-Techniken (Foucault 1994) wirken.

Überwachte		
Überwacher	**Organisationen**	**Individuen**
Organisationen	1. Oversight	3. Sousveillance
Individuen	2. Surveillance	4. Peer Monitoring

Abbildung 1: Rollen der Überwachung (aus: Bennett 2008, 12)

Diese Handlungsfelder zeichnen sich durch die Praktiken der Sammlung von Informationen und deren Kategorisierung sowie die Überprüfung von Personen aus, welche möglich sind aufgrund asymmetrischer **Herrschafts- und Machtverhältnisse**, manifestiert in der Verfügbarkeit entsprechender Technologien, Verfahren, zu Zwecken ihrer Lenkung, ihres Managements und ihrer Inklusion/Exklusion. **Datenschutz** stellt die Verregelung dieser Handlungen in Bezug auf dabei betroffene Informationsflüsse

im Allgemeinen dar, in denen die **Privatsphäre** als zu schützendes Gut eine zentrale Stellung einnimmt. **Sicherheit** als normierter Zustand und als Konstrukt gesellschaftlicher Aushandlungen dient als Argument für Überwachung und Kontrollen, während jene auch gänzlich ohne einen Verweis auf Sicherheit auskommen können.

Überwachung und Kontrolle stehen als Handlungen für sich. Im Zusammenhang mit Sicherheit als Argument allerdings ergibt sich eine vielfältige Dynamik, die u.a. mit den möglichen Konsequenzen konstruierter Normen und scheinbar unangreifbarer Argumentationslogiken zusammenhängt. Vor diesem Hintergrund ist die weitere Analyse der Expertise zu lesen.

3. Überwachung: Stand der Forschung und aktuelle Diskussionen

Jenseits der grundlegenden Definition von Überwachung als *Phänomen der Schaffung, Steuerung und Erhaltung gesellschaftlicher Ordnung* lässt sich feststellen, dass Überwachung in vielfältigen Formen Teil der Gesellschaft, des Alltagslebens sowie politischer Strategien und technologischer Anwendungen ist. Lyon (vgl. Bauman & Lyon 2013, 11) spricht davon, dass Überwachung eine zentrale Dimension der modernen Welt geworden ist. Die Themen anhand derer Überwachung erforscht und verhandelt wird sind vielfältig: vom Internet, sozialen Medien und der allgegenwärtigen Kontrolle unsers digitalen Lebens, über die verschiedenen theoretischen Ansätze, aber auch zu Umwelt, Gender, den Sport (z.B. Dopingkontrollen), das Militär, den Körper, Strafrechtspraxen , Umwelt, Flughäfen, *smart cities* bis hin zu historischen Analysen lassen sich Analysen und Studien finden, die Überwachung als Hauptfokus oder Folie der Forschung nutzen. Diese Bandbreite lässt sich u.a. auch anhand eines der führenden wissenschaftlichen Journals zu dem Thema exemplarisch zeigen. Die thematischen Ausgaben orientieren sich u.a. an folgenden Themen: *Gaming*, *Kindheit*, *Sport*, *Cybersurveillance*, *Gender*, *Widerstand*, *Foucault*, *Arbeit*, *CCTV*, *smarte Grenzen*, *Ungleichheit*. Der Inhalt einer nicht thematisch fixierten[4] Ausgabe steht hier exemplarisch:

- Keith Guzik: Discrimination by Design: Data Mining in the United States's 'War on Terrorism'
- Shelly Ikebuchi Ketchell: Carceral Ambivalence: Japanese Canadian 'Internment' and the Sugar Beet Programme during World War II
- Nicholas Holm: Watching the Paranoid: Conspiracy Theorizing Surveillance
- Christopher Gad, Peter Lauritsen: Situated Surveillance: an ethnographic study of fisheries inspection in Denmark
- Patrick O'Byrne, Dave Holmes Public Health STI/HIV Surveillance: Exploring the Society of Control

Die Bandbreite der Literatur zu Überwachung und Kontrolle spiegelt diese Vielfalt, wobei einige Themen, z.B. Videoüberwachung, Internet (Facebook) oder Datenschutz prominenter als andere sind. In der obigen Auswahl finden sich eine historische Analyse, eine Ethnographie, zwei mehr oder weniger theoretische Texte sowie eine Studie, die das Design von Technologie im weitesten Sinn untersucht. Zwar umreißt

[4] Vgl. Surveillance and Society, Vol 7, No 1 (2009) *http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Open%202009*

diese Auswahl sowie das Journal insgesamt das Feld der so genannten *surveillance studies*, welche – zusammengehalten von dem Fokus der Betrachtung von Überwachung – ein thematisch und disziplinär offenes Feld beschreiben. Doch fehlt weitgehend eine verbindende Theorie, die explizit als Theorie der Überwachung daherkommt. Ob dieser Mangel ein Nachteil ist, ist damit nicht gesagt. Die Suche danach kann sich aber schwierig gestalten. Leichter ist es nach den dominanten theoretischen Modellen zu schauen, die sich immer wieder in Variationen oder erneuerten Entwürfen vorfinden lassen: Die *Disziplinargesellschaft* und ihr Nachfolger die *Kontrollgesellschaft*. Diese Ansätze haben maßgeblich die Diskussion seit 20 Jahren bestimmt. Das ist insofern interessant, als dass die Analyse von James Rule von 1974 (*Private lives, public surveillance. Social control in the computer age.*) noch voll und ganz auf dem Begriff der sozialen Kontrolle aufgebaut war, mit den beiden genannten Ansätzen, nun neue Betrachtungsweisen eingeführt worden sind, die unvergleichbar dominant waren und sind. Sucht man also nach den theoretischen Fundierungen vieler Analysen von Überwachung, dann findet man sie in diesen theoretischen Konzepten. Deshalb sollen in der Folge diese beiden Ansätze kurz skizziert und ihre Bedeutung für die theoretische Betrachtung von Überwachung herausgestellt werden, insbesondere im Bezug zur vorliegenden Expertise. In Ergänzung wird noch die Denkrichtung der flüchtigen Moderne aufgeführt, die nicht gänzlich im Kontrast zu den anderen steht, ihr theoretischer Fokus aber andere Dinge adressiert.

3.1.Theorie der Überwachung

3.1.1 Panopticon vs. assemblage/Netzwerk

Die beiden dominanten Ansätze in der theoretischen Betrachtung von Überwachung und Kontrolle sind die des *Panopticon* auf der einen und der einer *surveillant assemblage* auf der anderen Seite. Diese theoretischen Perspektiven hängen entsprechend mit den Begriffen *Disziplinargesellschaft* und *Kontrollgesellschaft* zusammen und sind auf die Theoretiker Michel Foucault und Gilles Deleuze zurückzuführen. Insbesondere das Bild des Panopticon, welches Foucault in seinem Buch *Überwachen und Strafen* von 1976 als Erklärungsmodell nutzt, hat in der Überwachungsdiskussion eine enorme Wirkung entfaltet. Das Panopticon geht auf eine Idee des britischen Sozialreformers Jeremy Bentham zurück, der ein ideales Gefängnis skizzierte, in dem der Wärter von einem zentralen Punkt aus alle Gefangenen einsehen und überwachen konnte, diese aber im Gegenzug nicht den Wärter. Aus dieser asymmetrischen Situation des Sehens und der Sichtbarkeit heraus, folgerte Bentham, dass die Gefangenen, da sie nie wussten, ob sie beobachtet wurden oder nicht, sich selbst an die auferlegten Normen halten würden, sozusagen durch Selbstdisziplin. Bentham ging es bei dieser Architektur darum, die Insassen zu besseren Menschen zu erziehen, etwas das bis dahin im Strafvollzug eher

die Ausnahme war (Krause 1999, Foucault 1994; Whitaker 1999; Kammerer 2008). Foucault übertrug in seiner Analyse dieses Prinzip auf die Gesellschaft und ihre Institutionen in der Moderne. Das Sichtbarkeits- und Disziplinarregime des Panopticon ließ sich in Fabriken, Schulen, der Armee, und dem modernen Wohlfahrtsstaat insgesamt wiederfinden. Seine beiden tragenden Pfeiler waren die Aspekte der Fürsorge und der Kontrolle (Lyon 2001), die in der Analyse von Überwachung auch wie zwei Pole eines Kontinuums betrachtet worden sind. Die Antwort zur Bewertung einer Überwachungsmaßnahme lag dann darin festzustellen, wo auf einem solchen Kontinuum sich diese befand. Das Panopticon ist ein Synonym für eine Machtbeziehung, die vor allem zentralistisch organisiert ist und auf die durch Überwachung evozierte Selbstdisziplinierung abzielt. Obwohl das Panopticon, so wie es Bentham entworfen hat, nicht gebaut worden ist, hat die Idee sowohl im Strafvollzug – denn verschiedene Gefängnisse nahmen sich durchaus ein Beispiel an dem Modell – als auch in der Theorie über die Gesellschaft der Moderne einen zentralen Platz eingenommen, insbesondere über die Art sowie die räumlichen Kontexte von Überwachung. Die moderne sich herausbildende Gesellschaft des 19. und 20. Jahrhunderts konnte unter diesen Prämissen als in sich und ihren Institutionen panoptisch bezeichnet werden. Überwachungstechnologien wurden dann entsprechend auch als Verlängerung dieser Machtkonstellationen gesehen, insbesondere die Videoüberwachung. Aber auch das Internet und digitale Medien werden häufig als digitales Panopticon bezeichnet (vgl. z.B. Dupont 2008; Leistert & Röhle 2012; Bidlo 2011; Frischling 2014). Das Panopticon ist nach wie vor ein starkes Symbol, das im Zusammenhang mit Überwachung verwendet wird – teils unkommentiert, teils als Erweiterung der originären Idee: Superpanopticon, Post-Panopticon, Banopticon u.v.a.m. (vgl. Haggerty 2006, 26; Simon 2005). Diese alternativen Konzepte zum Panopticon sind vielfältig – variieren oder verwerfen jedoch das ursprüngliche Modell nur. Beschrieben werden weitgehend nur Formen und Modi der Überwachung in Variationen, die im Original-Panopticon nicht erfüllt sind oder hiermit erweitert werden. So hilfreich sie auch sind, um Überwachung in bestimmten sozialen Kontexten und Formationen zu erklären und die panoptischen Grundannahmen des Gefängnismodells umzukehren, zu erweitern oder mit neuen Ansätzen der sozialen Wirklichkeit näher zu bringen, sie erklären selten Grundlegendes zu Überwachung – also worum es im Kern geht, unabhängig von einer Technologie, einer Regierungsform oder einer gesellschaftlichen Formation.

Allein durch den informationstechnischen Sprung, den Computer spätestens gegen Ende der 1960er Jahre ermöglichten, hat Überwachung sich zu etwas entwickelt, das sich Jeremy Bentham noch nicht hätte vorstellen können. Es ergaben sich nun neue Möglichkeiten Daten zu erfassen, auszuwerten und ordnungstechnisch einzusetzen. Überwachung wandelte sich von der direkten und disziplinierenden Kontrolle, wie sie noch im Panopticon ersonnen wurde, hin zu einer Überprüfung von Kategorien,

Maßnahmen, Personengruppen und vordefinierten Szenarien. Und auch moderner Strafvollzug ist an dem Menschen interessiert, sofern er sich an der Resozialisierung der Subjekte orientiert, auch durch die Einübung von Disziplin. Für ein Verständnis von Überwachung ist es wichtig zu verstehen, inwiefern das Panopticon und dessen nachwirkendes Erklärungspotenzial auf den Menschen gerichtet war, auf seine Seele, auf die Internalisierung von Verhaltensweisen.

Zusammengefasst kann man sagen, dass das Panopticon in so genannten Einschließungsmilieus operiert, in denen durch Zwang, Selbstdisziplin, Fürsorge und Überwachung Menschen bzw. Individuen zu passenden Mitgliedern der Gesellschaft geformt werden. Macht ist zentralistisch organisiert und sie bedient sich verschiedener Regierungstechniken, um diese zu erhalten. Disziplin ist eine solche Technik, die so wirksam ist, weil sie Zwang über die Körper selbst vermittelt und sich in diese einschreibt. Das Panopticon Benthams dehnt sich auf die ganze Gesellschaft aus, die Idee von Fürsorge und Kontrolle wird zum leitenden Prinzip. Foucault kombiniert im Anschluss daran zwei Dinge, die wesentlich sind für viele Formen der Überwachung: Wissen und Macht – wobei Überwachung sich aus der Kombination der beiden in unterschiedlichen sozialen und institutionellen Konstellationen ergibt. Bei Foucault ist es vor allem der zentrale Blick, der durch die gestörte Reziprozität zur Selbst-Disziplinierung des Insassen oder der Objekte des überwachenden Blickes wird.

Eine Erweiterung dieser Idee einer Disziplinargesellschaft ist das Konzept der Kontrollgesellschaft, welche die Ideen des Zwangs, der Einschließungsmilieus und vor allem der zentralen Kontrolle verlässt. Der Bruch, wenn man es denn so nennen will, zwischen der Foucaultschen Disziplinargesellschaft und einer Kontrollgesellschaft nach Deleuze (vgl. dazu Kammerer 2008, 2011), ist am ehesten mit der Digitalisierung von Überwachung eingetreten, zumindest aber ist der Bruch dort eingeleitet worden. In der Deleuzeschen Kontrollgesellschaft wird die Kontrolle nicht mehr zentral und disziplinierend, sondern de-territorialisiert und die Kontrolle nicht auf Zwang, sondern durch Verführung begründet (Lyon 2006; Bogard 2006; Kammerer 2008). Die *surveillant assemblage* (Haggerty & Erison 2000; Bogard 2006) ist das prägende Bild dieser Art von Überwachung – verstanden als eine Maschine, welche menschliche Körper von ihren räumlichen Fixierungen löst und in eine Reihe unterschiedlicher, separater Ströme wandelt. So transformiert existieren Menschen dann als Daten-Double oder Hyper-Realität (Bogard 1996) in einer Netzwerkstruktur informationstechnischer Apparate, in denen Sinn dann erst wieder neu und beliebig re-kombinierbar geschaffen wird. (vgl. Lyon 2007; Haggerty 2006; Bogard 2006). Ob und inwiefern ein Bruch tatsächlich vollendet worden ist, ist unklar, wenn sich eine solche scharfe Trennung jenseits der Theorie tatsächlich finden lässt. Vielmehr deutet einiges eher darauf hin, dass beide Modi der Überwachung nebeneinander her und vermischt mit einander existieren.

Mit dem Konzept einer Kontrollgesellschaft wird auch auf die Offenheit von Gesellschaft verwiesen, in der diese Kontrollen stattfinden. Die vorausschauende Kontrolle ist dabei ein zentraler Punkt. Das ist mit den Begriffen der Hyper-Realitäten gemeint: die vorauseilende Risikokontrolle, das Ausschließen von möglichen Gefahrenszenarien soweit im Vorwege, dass ein Einschreiten angesichts tatsächlicher Gefahren überflüssig wird (vgl. Bogard 1996, 2006). Räumliche Bezüge werden hier über die Risikoräume einer simulierten Überwachung hergestellt. Sie können in der Konsequenz Diskurs-steuernd wirken. So geschaffene räumliche Anordnungen sind elementar für Überwachungspraktiken, da über sie Ein- und Ausschlüsse definiert werden. Denn die Beschaffenheit der Räume definiert auch den Kreis der überwachten Zielpersonen bzw. die Risikogruppe, die es im Vorwege abzuwehren gilt.

Die wesentlichen theoretischen und konzeptionellen Unterschiede beider Ansätze bringt Kammerer auf den Punkt, wenn er festhält, dass die Kontrollgesellschaft nicht das Ende von irgendwas ist (hier der Disziplinargesellschaft), sondern das Ende des Enden-Könnens. In der Disziplinargesellschaft hört man nie auf anzufangen (Schule, Kaserne, Fabrik etc.), während man in der Kontrollgesellschaft nie mit etwas fertig wird. Die Techniken der Kontrolle zeichnen sich dadurch aus, dass sie permanent und in kontinuierlicher Variation vorkommen (vgl. Kammerer 2011, 31). Es gibt nichts verlässliches mehr, man muss ständig bereit für eine Überprüfung sein – eine Abwägung aus Fürsorge oder Kontrolle existiert nicht mehr, ein übergeordneter Zwang ebenfalls nicht, sondern nur die beständige Überprüfbarkeit anhand oftmals unklarer Regeln, Klassifikationen und Bewertungsraster. Der Algorithmus wird zur Schlüsseltechnologie bei der Überprüfung möglicher zukünftiger Szenarien in der Gegenwart. Während die Disziplinargesellschaft über Zwang Sicherheit herstellt, basiert die Kontrollgesellschaft auf beständiger Unsicherheit der Individuen einer Überprüfung nicht standzuhalten.

3.1.2 Die flüchtige Moderne, Risiko- und Sicherheitsgesellschaft

Kontrolle durch Verunsicherung zu schaffen mag angesichts vieler Programme zur Sicherheitsforschung geradezu paradox erscheinen. Dennoch liegt hierin ein Schlüssel auch zur Betrachtung von Überwachung als Rahmung technischer Innovationen im Bereich Sicherheit und von theoretischen Ansätzen, die der Kontrollgesellschaft einen sozialen und politischen Hintergrund geben. Kern dieses sozio-politischen und damit auch analytischen Hintergrundes ist der Wandel der Moderne, wie er sich spätestens seit den 1970er Jahren in Westeuropa und den USA feststellen lässt. Er ist Grundlage für eine Vielzahl von Gesellschaftsanalysen, die in der Folge immer neue Beschreibungen hervorgebracht haben. Die für diese Expertise relevantesten Modelle sind zum einen die Risikogesellschaft, die nach Beck auf der Freisetzung der Individuen aus den tradierten Formen sozialer Ordnung – wie Familie, Klasse, Schicht usw. – beruht (*mit Foucault könnte man hier in Bezug auf Überwachung und Kontrolle durchaus auch von*

Einschließungsmilieus sprechen) (vgl. Beck 1986, 115). Technische und gesellschaftliche Risiken nehmen zu, werden produziert und sind inhärenter Teil (post-)moderner Gesellschaften. Weiterhin kennzeichnend sind in einer Risikogesellschaft auch die Prozesse der Entgrenzung auf zeitlicher, räumlicher und sozialer Ebene. Lange bestehende Sicherheiten (z.B. in Form lebenslanger Arbeits- oder Familienverhältnissen u.ä.) erodieren. Das Schadenspotenzial von Risiken ist in diesen Dimensionen demnach nicht mehr begrenzt, es kann jeden und alles treffen. Vernetzung und weitgehende (und nicht immer zu durchschaudende) Wechselwirkungen sind bestimmend für die Gesellschaft. Eine Zurechnung der Verursacher von Risiken wird zunehmend schwieriger, womit auch klare Verantwortungen verschwimmen. Die Risikogesellschaft ist somit eine Gesellschaft, die Katastrophen zu antizipieren versucht und hierdurch Handlungspotenziale generiert.

Bauman (2003) hingegen spricht von einer flüchtigen Moderne, in der die Unsicherheit zum zentralen Aspekt sozialen Lebens wird. Deregulierung sowie Privatisierung sind die Kennzeichen, unter denen gesellschaftliche Prozesse stattfinden. Die flüchtige (im Englischen: *liquid*) Moderne zeichnet sich ebenfalls durch eine Veränderung der Verhältnisse aus, dem Verlust tradierter Sicherheiten, einer Hinwendung zum eigenverantwortlichen Subjekt, das auf sich selbst zurückgeworfen, nicht mehr die Selbstverständlichkeiten einer Wohlfahrtsgesellschaft zurückgreifen kann. Macht ist nicht mehr fassbar, wie in einer panoptischen Gesellschaft, sondern überall und nirgends, wenig greifbar und somit für die Subjekte „flüchtig“, ungreifbar, oft dadurch nicht adressierbar. Willkür und Undurchschaubarkeit sind mögliche Folgen. Außerdem ändert sich der generelle Charakter von Gesellschaft und gesellschaftlichen Beziehungen.

Alles wird zu einer Ware, auch die Sicherheit, die man sich in einem Umfeld genereller Unsicherheit bzw. gesellschaftlicher Verunsicherung kaufen kann. In einer Konsumgesellschaft wie sie Bauman entwirft, muss jeder ständig seine Fähigkeiten auffrischen und optimieren, um zu bestehen (Bauman 2009, 21). Es ist das Bild von zutiefst individualisierten Gesellschaften, in denen jeder für sich selbst den gesellschaftlichen und lebensweltlichen Risiken ausgesetzt ist, und damit beständig Risikoanalysen machen muss. Da scheint es geradezu widersprüchlich zu sein von einer Sicherheitsgesellschaft zu sprechen, wie es Stolle und Singelnstein (2008) in dem gleichnamigen Buch tun. Doch ihre Analyse zur sozialen Kontrolle im 21. Jahrhundert (*so der Untertitel des Buches*), setzt genau an den Wandlungen der Moderne an, die von Bauman und Beck (Bauman 2003, Beck 1986) angesprochen worden sind. Ihr Kernargument ist, dass gerade die Veränderungen der Gesellschaft, – spürbar in den Arbeitsprozessen, den sozialen Bindungen, traditionellen Institutionen der Vergesellschaftung oder Beschäftigungsverhältnissen – die in ihrer Struktur eben gerade die Verunsicherungen des Einzelnen hervorrufen (können), auf der anderen Seite eine

verbesserte Sicherheitsarchitektur verlangen. Und damit ist nicht wie bis zum Ende des Kalten Krieges das Militär gemeint, sondern nun geht es primär um innenpolitische Prozesse. Diese sind selbstverständlich heutzutage an globale Entwicklungen gekoppelt. Dennoch bezieht sich Sicherheit nun auf die Sicherheit des Bürgers, aber auch auf die Sicherheit des Staates vor dem Bürger, der in seiner Unsicherheit – zumindest bezogen auf bestimmte Gruppen – zu einer Gefahr für ersteren werden kann (Legnaro & Birenheide 2008, Wacquant 2009, Garland 2008). Der Blick von Stolle und Singelnstein konzentriert sich auf die Instrumente sozialer Kontrolle, auf das Strafrecht und die damit einhergehenden Entwicklungen auf diesem Gebiet – nicht nur für Deutschland, sondern für Westeuropa, die USA und die weitere Welt. Der Sicherheitsapparat wird dort als eigenständiger Akteur aufgefasst, der seine Befugnisse beständig ausweitet und zum Teil privatisiert agiert – private Gefängnisse in Großbritannien oder den USA, aber auch in Deutschland wären Beispiele dafür. Auch, und dieser Aspekt ist vor allem im Hinblick auf diese Expertise von großer Bedeutung, bedient sich der Sicherheitsapparat der Mobilisierung von Öffentlichkeit mit dem Ziel diese mit eigenen Interpretationen von Kriminalitätsraten, Unsicherheitsfaktoren und der Gefährdung des öffentlichen, zivilen Lebens zu beeinflussen (vgl. ebd. 2006, 49ff). Sicherheitsinstitutionen würden eine eigene Sicherheitspolitik betreiben, weshalb auch von einer Sicherheitsgesellschaft gesprochen werden könne. Insbesondere der Aspekt der vorausschauenden Kontrolle gewinnt unter diesen gesellschaftlichen Bedingungen eine neue Qualität und Prominenz.

Die Überwachung in einer solchen Sicherheitsgesellschaft, deren Beschaffenheit der einer Risikogesellschaft oder der flüchtigen Moderne Baumans ähnelt, ist die logische Konsequenz, die sich aus der Freisetzung von Arbeitskräften, der Produktion von Unsicherheiten (vgl. Monahan 2011) und den so entstandenen gefährlichen, unerwünschten, nicht mehr benötigten Menschen oder ganzer Gruppen (die man als solche kategorisiert) ergibt. Die Beherrschung von Gesellschaft ist anders nicht mehr vorstellbar, wenn andere „Verträge“ in der Gesellschaft, die auf Zusammenhalt, gemeinsame Ziele und Solidarität aufgebaut sind, fehlen bzw. mehr und mehr irrelevant geworden sind. Mal sind es die neoliberalen Regimes (Stolle & Singelnstein benutzen diesen Begriff; auch Briken & Eick 2013), mal der Konsumismus einer flüchtigen Moderne, der diese Individuen produziert – immer scheinen die Lösungen allerdings in einer Abwehr dieser Menschen und Gruppen zu bestehen (vgl. Baumann & Lyon 2013; Monahan 2011; Stolle & Singelnstein). Bereits Beck beschrieb den Mechanismus, der unter den gewandelten Bedingungen und Strukturen von Gesellschaften zu einem Kernelement wird, nämlich dass „der Ausnahmezustand zum Normalzustand zu werden droht“ (Beck 1986, 31; zum Thema Ausnahmezustand und Sicherheit vgl. auch Lüdtke & Wildt 2008). Bei Beck war es die Risikogesellschaft, die zu einer katastrophalen Gesellschaft geworden war – aber auch in der Sicherheitsgesellschaft oder der Überwachungsgesellschaft ist das Risiko eine zentrale Größe, grundsätzlich zwar

berechenbar, und darum auch als Argument nutzbar, um diesen Risiken zu begegnen. Die Frage allerdings ist, ob nicht Risiko und Gefahr verwechselt werden, wenn die Risiken so beständig und der Gesellschaft scheinbar so unvermittelbar sind, dass die Überwachung und Kontrolle sich auf alles und jeden auszudehnen droht. Überwachung, so die Schlussfolgerung aus den Kernaussagen der flüchtigen Moderne, ist zu einem reinen Herrschaftsinstrument mutiert, in dem der Aspekt der Fürsorge (Lyon) keine Rolle mehr spielt, sondern die Prävention gegenüber der Reaktion an Bedeutung gewinnt.

3.1.3 Zusammenfassung: Theorie der Überwachung

Die drei hier nur kurz umrissenen Ansätze sind eigentlich keine Theorien der Überwachung, sondern Theorien der Gesellschaft, in denen Überwachung als Katalysator eine zentrale Rolle spielt. Sie sind der Hintergrund, vor dem Überwachung als Umstand an sich und in ihren Erscheinungen zu bewerten und zu analysieren ist. Überwachung als Konglomerat von Handlungen muss solchen Annäherungen verhaftet bleiben. Die Rolle des Handelns, seine Erscheinungsweisen, Kennzeichen und Dynamiken werden somit jeweils unter anderen Bedingungen beleuchtet. Diese hier vorgenommene Abgrenzung dient zunächst hauptsächlich der Übersichtlichkeit. Denn jede der Theorien bzw. soziologischen Ansätze ist hinreichend kompliziert und folgt einer in sich geschlossenen Logik, die es herauszustellen gilt. Als Gesamtpaket betrachtet sind diese Ansätze und die dahinter stehenden gesellschaftlichen Dynamiken eher ineinander verwoben als voneinander getrennt. Zusammen betrachtet stellen sie dann einen hinreichend umfassenden soziologischen Hintergrund für die Bedeutung und die Zusammenhänge von Überwachung in Gesellschaften in vielen ihrer Aspekte da. Nicht für sich, sondern im Ensemble wird deutlich, welcher Nutzen sich hieraus ziehen lässt.

Das **Panopticon** verweist auf zweierlei: Den **Zwang** sowie die **Sichtbarkeit**, als dessen zentrales Mittel. In seiner ursprünglichen Idee war das Panopticon ein Gebäude zur Besserung der Menschen, die von der Gesellschaft bzw. dem Staat als abweichend betrachtet wurden. Dort wurden sie resozialisiert und wieder für die Gesellschaft nutzbar gemacht. Als Chiffre für Machtverhältnisse wurde daraus im Anschluss an Foucault ein Bild und Analysewerkzeug für das Verhältnis von Gesellschaft und Individuum insgesamt. Überwachung als Beobachtung, die zu einer Selbstdisziplinierung führt, weil bei Normverstoß eine Sanktion befürchtet wurde, ist zentral in diesem Modell. Sichtbar sein, sich nicht den Blicken entziehen zu können ist die operationale Logik in dieser klassischen Moderne, verbunden mit Industrialisierung und Wohlfahrtsstaat. Auch die **Kontrollgesellschaft** will, dass ihre Mitglieder verfügbar sind, sich nützlich machen. Aber sie verlagert diese Aufgabe auf die Individuen selbst. Die **Selbstdisziplin** wird nicht durch **Zwang** erzeugt, sondern durch **Verführung**.

Sichtbarkeit ist nicht zentral, sondern ein Beständiges sich anpreisen, an sich arbeiten – ohne garantierten Erfolg. Ständig erfolgt eine Überprüfung und es wird aussortiert. In- und Exklusion durch Kontrollen in einer auf den Markt und den Konsum fixierten Gesellschaft sind der Schlüssel zum Verständnis. Man selbst wird zum Konsumgut. Während die Disziplinargesellschaft sich durch Fürsorge und eine Reaktion auf Fehlverhalten auszeichnete, setzt die Kontrollgesellschaft auf Prävention – was auch die mögliche präventive Exklusion möglicherweise Risiko-behafteter Individuen oder Gruppen einschließt. Die Sicherheitsgesellschaft ist eine **Präventionsgesellschaft**, strafrechtlich vor allem, aber auch in Bezug zu dem Bedürfnis, möglichst alle Risiken weit im Vorwege auszuschalten.

Beck, Bauman und andere Vertreter, die einen **Wandel innerhalb der Moderne** festgestellt haben, bieten mit ihren Analysen der Risiko-, Sicherheits-, oder flüchtigen Moderne die dafür grundlegenden Gegenwartsanalysen, in denen sie die Zusammenhänge aufzeigen und die Funktionslogiken offenlegen (vgl. auch Latour 2009, Gugerli 2009). Dass diese theoretischen Modelle auch heute kaum in Reinform vorkommen, ist offensichtlich. Dennoch lassen sich durch diese Analysemodelle bestimmte Entwicklungen trennschärfer betrachten, ohne ständige Ausnahmen und Einschränkungen vornehmen zu müssen.

3.2 Theorie in der Praxis von Überwachung

So sehr die Modelle einer Überwachungs-, Kontroll-, oder Risikogesellschaft die gesellschaftlichen Grundprinzipien erhellen können, so wenig können sie die Vielfalt der Umstände, in denen Überwachung stattfindet, erklären. Überwachung als Phänomen und Handlung ist zu vielfältig um im Einzelnen allein mit diesen Modellen beschrieben zu werden. Das beginnt schon damit, dass eine sinnvolle Unterscheidung zwischen der massenhaften Überwachung à la NSA und der gezielten Überwachung einzelner Personen gemacht werden muss, wie sie beispielsweise als gängiges Instrument kriminalpolizeilicher Arbeit (oder einer geheimdienstlichen Tätigkeit klassischer Form, vgl. APuZ 18-19/2014) vorgenommen wird. Auch hier gibt es Bereiche der Überschneidung, aber generell lassen sich diese beiden Bereiche sehr wohl trennen. Die Unterscheidung hier liegt u.a. in der Art und Weise wie Verdacht konstruiert wird (vgl. Kriminologisches Journal 46/3). Eine Massenüberwachung geht prinzipiell davon aus, nicht zu wissen wer gesucht wird, sie verfügt nur über vage Anhaltspunkte und Vorstellungen davon, was verdächtig sein kann. Die gezielte Überwachung einzelner oder kleinerer Gruppen geht von einem Verdacht aus und überprüft diesen. Ob die jeweilige Maßnahme strikt mit den großen Modellen zu analysieren und adäquat zu bewerten ist, ist zweifelhaft. Viel eher lohnt sich ein Blick auf Überwachung (und Kontrolle) mit nicht so weit gefassten Modellen, die sich dafür genauer mit den Erscheinungsformen auseinandersetzen. Dabei geraten dann auch andere Aspekte

wieder in den Fokus, mit denen eine genauere Analyse vorgenommen werden kann. Das bedeutet nicht Überwachung nur als Folge oder im Zusammenhang mit spezifischen Technologien und Verfahren zu untersuchen, sondern generell andere Modelle und soziale Konstellationen zu beachten sowie auf einzelne Aspekte gesondert zu schauen. Die Rolle von Daten, die in der Definition zu Datenschutz bereits angerissen wurde, soll hier den Anfang machen, da die Verfügbarkeit von Daten und die Methoden ihrer Verarbeitung diese zu einem der wichtigsten Grundstoffe für Überwachung gemacht haben. Die digitalisierte Überwachung ist gegenwärtig und höchstwahrscheinlich auch in der Zukunft die vorherrschende Form der Überwachung, womit nicht gesagt ist, dass es sich hierbei um eine einheitliche Entwicklung handelt (Graham & Wood 2003, Langheinrich & Mattern 2003, Kawashima 2008, Caputo 2010, Naik & Lad 2014).

3.2.1 Big Data – Kategorien zur Kontrolle der Welt

Big Data als technisches Konzept sowie als Diskurs des Umganges mit den Folgen der Digitalisierung von Gesellschaft ist ein wichtiger Aspekt gegenwärtiger Diskussionen. Das gilt sowohl für viele Unternehmen, die den Schatz an Daten heben wollen, um ihre Produkte oder Dienstleistungen zu verbessern, als auch für öffentliche Verwaltungen, die so mehr über den Bürger erfahren können, um ein besseres Management von Städten und Infrastrukturen vorzunehmen. Letztlich interessieren sich selbstverständlich auch die Geheimdienste, Polizeien und andere so genannte Sicherheitsagenturen für die vorhandenen Daten. Und schließlich hat der Begriff Big Data auch in der Forschung zu Überwachung ein neues Feld eröffnet, welches sich nun mit dem Thema und den Praxen darum befasst (Cukier & Mayer-Schönberger 2013; Geiselberger 2013; Andrejevic & Gates 2014; Müller-Quade 2014).

Daten also sind der Stoff, aus dem Überwachung in der flüchtigen Moderne gemacht ist. Aber wie funktioniert das? Und warum ist das alleinige Vorhandensein der Informationen an sich noch keine Überwachung? Es ist unbestreitbar, dass gegenwärtige Formen der Überwachung und Kontrolle vor allem auf die Verfügbarkeit von Daten angewiesen sind. Aber ist damit – wie es manchmal erscheint – jeder Austausch von Informationen gleich eine Überwachung, jedes Datum ein Skandal? Der Schlüssel dafür liegt tiefer als nur in den Informationen selbst.

Kommunikation von Informationen und Daten ist zunächst etwas, das für das menschliche Leben und ein gesellschaftliches Leben von grundlegender Bedeutung ist. Ohne einen Austausch von Informationen zwischen den Mitgliedern einer Gruppe oder Gesellschaft ist kein soziales Leben denkbar. Über das Sammeln, Austauschen und Bewerten von Informationen versuchen Menschen sich innerhalb ihrer Umwelt zurecht zu finden bzw. die sie umgebende Welt überhaupt zu begreifen. Die Informationen oder Daten werden z.B. genutzt, um festzustellen, wer jemand ist, wo eine Person herkommt oder mit welcher Absicht sich jemand an einem Ort aufhält, der auch von anderen

Gruppen beansprucht wird. In solchen Fällen geht es um die Identität des jeweils anderen, zur eigenen Sicherheit oder auch nur um die Möglichkeit zu besitzen eine Beziehung zu diesem Menschen aufzubauen. Der Umgang mit Informationen beruht grundsätzlich darauf, dass Informationen bewertet werden. Informationen über die Welt und die dazugehörigen materiellen und nicht-materiellen Dinge und Erscheinungen werden kategorisiert und klassifiziert, um sie mit Bedeutungen und Sinn zu versehen. Damit handelt es sich dabei um eine zutiefst menschliche Eigenschaft (Bowker & Star 1999), die es ermöglicht auch in einer fremden Umwelt auf Muster zurückzugreifen, mit denen Neues und Altes sinnvoll geordnet werden kann. Kategorien oder Klassifizierungen bestimmen z.B. über gut-böse, essbar-giftig, groß-klein, schön-hässlich usw.. Kategorien müssen nicht immer extreme Paare sein, sondern es kann sich auch um Abstufungen handeln, Einteilungen, in denen Merkmale unterschieden werden oder Definitionen, die sagen wie etwas beschaffen ist, das für einen bestimmten Zweck nützlich, wichtig oder überflüssig ist. Alle Klassifikationen und Kategorien sind von Menschen gemacht. Jede Definition beruht auf von Menschen verabredeten Definitionen, mit denen Grenzen zu anderen Erscheinungen, Dingen oder sozialen Gruppen gezogen werden. Und wer die Macht hat, diese Definitionen zu beeinflussen hat auch die Macht über die Kategorien. Vereinfacht könnte man sagen, dass die Macht darüber zu bestimmen, wie etwas aussieht oder was in eine Kategorie fällt oder nicht, bedeutet, Kontrolle darüber auszuüben in welche Weise die Welt wahrgenommen wird.

Übertragen auf die täglich bei uns anfallenden Daten und ihre mögliche Kategorisierung bedeutet das, dass weniger die Daten als solche das Problem sind, sondern die Kategorien, mit denen sie bewertet werden. Denn erst durch diese erhalten die Daten einen Sinn und können in Bezug auf eine von anderer Seite gemachte Definition weiter verwendet werden. Wenn also ein Einkauf nicht nur bedeutet, dass eine Person Milch, Zucker und Mehl gekauft hat, sondern in der Logik einer Bewertung dieser gesammelten Daten, dass diese Person wohl gern Pfannkuchen isst, welche als nicht gesund eingestuft wären, dann ginge die Erhebung der Daten über eine Aufzählung der gekauften Dinge weit hinaus.

Die Macht darüber zu bestimmen, was einzelne Daten im Zusammenhang bedeuten, ermöglicht die Kontrolle bzw. Überwachung von Menschen, ohne dass diese anwesend sein müssen, noch müssen sie im Augenblick der Kontrolle von dieser wissen. Die Möglichkeit eine Definition zu bestimmen und durchzusetzen, bedeutet darüber zu entscheiden, wer Einlass erhält oder wer ausgeschlossen wird, weil die in der Definition vorgegebene Norm nicht erfüllt wird. Wer die Verfügungsgewalt über Daten und die Definitionsmacht über ihre Bewertung besitzt, kontrolliert die Möglichkeiten gesellschaftlicher Teilhabe. Eine informationelle Selbstbestimmung, die besagt, dass eine Person die Kontrolle über die Verwendung ihrer eigenen Daten haben soll, ist ohnehin nur noch eingeschränkt möglich. Gerade durch die digitale Vernetzung und

Abhängigkeit unseres sozialen, politischen sowie wirtschaftlichen Lebens, ist eine selbstbestimmte Verfügung und Bewertung der eigenen Daten immer weniger realisierbar. Somit entschwindet jedem einzelnen Bürger die Kontrolle über die Verwendung von Daten immer mehr. Für Strategien der Überwachung werden solche Kategorien und Klassifikationsmuster aber immer wichtiger und bilden heute das entscheidende Element von sozialer Kontrolle durch Staat und Wirtschaft.

Auch ohne Big Data hat es Überwachung im Sinne einer systematischen Kontrolle von Menschen wahrscheinlich in der einen oder anderen Form schon immer gegeben. Das Aufkommen einer rationalen Bürokratie, inklusive einer modernen Polizei im 18. und 19. Jahrhundert hat diese Überwachung jedoch systematisiert und institutionalisiert (Vgl. Giddens 1984; Weber 1972; Winkelmann & Förster 2007; Kammerer 2008; Zerback 2009). Apparate wurden geschaffen, mit denen Menschen überwacht, ausspioniert und kontrolliert werden konnten. Die Stasi der DDR ist das wohl umfassende Beispiel für diese klassische „alte" Form der Überwachung, die an Personen als Personen interessiert war (vgl. Giseke 2011). Zur Überwachung gehörten auch immer schon verschiedene Maßnahmen der Kriminalistik, um Personen an Merkmalen (wieder) zu erkennen, wie etwa die Geschichte des Fingerabdruckes oder der Verbrecherfotografie zeigt (vgl. Berchthold 2007, Kammerer 2008). Solche (Daten-) Sammlungen, in denen Merkmale, Ereignisse und Personen zusammengeführt werden konnten, sind für viele Überwachungspraktiken von entscheidender Bedeutung gewesen und heute der Kern der meisten Praxen, die als Überwachung beschrieben werden können. Die Möglichkeiten von Computern haben neue Formen der Überwachung geschaffen, die sich von den bisherigen darin unterscheiden, dass sie nicht länger an der Person als Person interessiert sind (vgl. u.a. Rule 1974, Marx 2002). Für solche neuen Formen der Überwachung sind die Zusammenhänge, in denen Daten abgegeben oder gesammelt werden, viel interessanter als die eigentliche Person, da generell eher die Gesellschaft als solche anhand der Daten, Filter und Kategorien unter Beobachtung steht. Eine solche Überwachung konzentriert sich auf die Merkmale und mögliche Zusammenhänge und sucht die Personen, die es zu überwachen gilt, erst aufgrund der jeweils passenden Daten heraus (vgl. Marx 2002). Das bedeutet aber, dass potentiell alle möglichen Daten von möglichst vielen Menschen gesammelt werden müssen – denn es ist ja völlig unbekannt wer wo überwacht werden soll und vor allem, ob ein Anlass zu direkter Überwachung besteht. Um eine effektive Kontrolle oder Überprüfungsmöglichkeit zu schaffen, bedarf es möglichst vieler verschiedener Daten und Merkmale, die zusammengeführt werden können – Big Data eben, um in die Zukunft zu schauen (vgl. Zurawski 2014). Diese Daten können aus persönlichen Daten stammen, aus biometrischen Merkmalen (Fingerabdruck oder DNA-Profile), Einträgen bei der Schufa, Einkäufen, die Art der Auslandsbesuche usw.. Überwachung bedeutet unter diesen Bedingungen eine ständige Risikoabschätzung und eine möglichst vorausschauende Kontrolle, um bereits im Vorwege maschinengesteuert eine Überprüfung

durchzuführen und Kontrolle auszuüben. Überwachung als Idealtypus bedeutet die Kontrolle möglicher Abweichungen von einer durch Daten und Kategorien erzeugten Norm. Das Bewusstsein davon kann in der Gesellschaft zu Konformität führen, die sich durch eine soziale Kontrolle so nicht ergeben würde, da jene wesentliche wandelbarer und durch die Gegenseitigkeit auch offener und flexibler gestaltbar wäre. Big Data ist vor allem vor dem Hintergrund einer Moderne, die von Flexibilisierung und der Rekombination der Wirklichkeit (vgl. Gugerli 2009, 13, 89f.) gekennzeichnet ist, für die Analyse von Überwachung zentral, wenn es nicht die Masse an Daten selbst ist, die diese Rekombinationsmöglichkeiten erst selbst geschaffen hat.

3.2.2 Überwachung als social sorting

Dieser Ansatz baut inhaltlich im Großen und Ganzen auf den gerade gemachten Argumenten auf. David Lyon hat diese Bezeichnung in der Überwachungsdiskussion etabliert und theoretisch entwickelt. Unter *social sorting* versteht Lyon die Form der Überwachung, die aufbauend auf Kategorien und Klassifikationen Stereotypen verstärkt soziale Unterschiede zementiert und Diskriminierung (positiv und negativ) als grundsätzliches Kriterium einer Auswahl nutzt (vgl. u.a. Lyon 2001, 47, auch 2002, 2003, 2007, 2014). Ausschlaggebend ist für ihn dafür die Computerisierung von Überwachung, basierend auf einer Informationsverarbeitung, die elektronisch, automatisch und vor allem intransparent verläuft. Soziale Ordnung bzw. die Hierarchisierung von Gesellschaft und darüber die Festlegung von Machtverhältnissen und Herrschaftskonstellationen beruht in zunehmenden Maß auf dieser Form der Überwachung. Überwachung bedeutet in diesem Fall die Einteilung von Menschen und Gesellschaften in Kategorien und ihrer bürokratische Erfassung mittels Datenbanken.

Bennett et al. (2014, 4) präzisieren diesen Ansatz in einer großen Studie zur Überwachungsgesellschaft in Kanada wie folgt:

> *Having a sense of control over our public persona is vitally important, as are the ways in which we are profiled and categorized, because such processes have an impact on our life chances and choices. We are treated differently depending on our profiles, and such treatment, in turn, changes our present and our future. This is social sorting.*

Diese Betrachtungsweise hat eine enorme Prominenz in den *surveillance studies* erlangt. Die Verwendung des Konzeptes in der Literatur zu Überwachung ist enorm, gleich ob es sich um Videoüberwachung an Schulen (Taylor 2011, 2013) handelt, oder um theoretische Betrachtungen (vgl. Simon 2005), Analysen zur Bedeutung von Identitätsausweispapieren (Lyon & Bennett sowie die Aufsätze darin 2008) oder um Arbeiten, die sich mit der Überwachung des Konsumverhaltens von Kunden beschäftigen (Marx 2002; Lyon 2003; Pridmore 2008; Zwick & Knott 2009; Zurawski

2011, 2014). Marx spricht im Zusammenhang mit der Überwachung bzw. des Monitoring der Kunden auch von einer *soft surveillance*, in der der Kunde/Bürger/Überwachte bei seiner Überwachung behilflich ist, indem Angebote gegen Daten getauscht werden (vgl.Marx 2006; Zurawski 2014b; IRiSS report WP4[5]). Zurawski nutzt in diesem Zusammenhang die Bezeichnung vom Konsum der Überwachung (2014a, 2014b), in der die Überwachung in die jeweiligen Aktivitäten eingebaut worden ist, aber eben nicht offen sichtbar ist und somit bemerkt werden kann.

Es geht bei diesem Ansatz also vor allem um die Möglichkeiten und Verfahren, durch die Menschen klassifiziert und eingeteilt werden, wodurch ihnen sowohl Chancen verwehrt, als auch ermöglicht werden können. Das ist nicht besonders neu und auch keinesfalls an eine Informationsverarbeitung durch Computer gebunden, aber durch diese enorm beschleunigt. Bowker & Star (1999) argumentieren, dass die Fähigkeit zu klassifizieren uns zu Menschen macht. Beispiele einer kritischen Forschung zu Statistiken oder zum Umgang mit Statistiken z.B. hinsichtlich eines Bevölkerungs-managements zeigen inwieweit hierüber Kontrolle ausgeübt werden kann und somit diese Verfahren auch eine Überwachung der Bevölkerung darstellen. Die Definition statistischer Merkmale, Klassen und Begriffe, ihre Zulassung und Verwendung ist ein Mittel der Macht. Denn was nicht adäquat erfasst werden kann, weil eine entsprechende Kategorie nicht vorhanden ist, existiert in diesem Sinne auch nicht. Axelsson & Sköld (2011), aber auch Graham (2005), sowie Browne (2010) zeigen dies an den Zusammenhängen von Demographie, Statistik und Identität. Die Datenbank ist somit in der Informationsgesellschaft die zentrale Technologie, wenn man ein *social sorting*, wie es Lyon formuliert, zum Kern der Betrachtung von Überwachung gemacht hat. Was dort wie gesucht wird, nach welchen Kriterien und wie generell Welt durch Datenbanken erfahrbar gemacht wird, hat Gugerli (2009) herausgearbeitet. Insbesondere vier Merkmale sind es, nach denen diese Datenbanken funktionieren bzw. wie sie sich zum Verstehen von Welt einsetzen lassen: Die Suche nach dem *Normalen* – nach der *Devianz* – nach dem *Muster* – nach der *Form.* Dass das Konzept des social sorting auch in prä-elektronischen Zeiten funktioniert hat, hat wiederholt Thompson gezeigt (u.a. 2006, 2008, 2014), insbesondere an verschiedenen Formen des Pass- und Kontrollwesens in den USA und Kanada (an historischen Beispielen von Alkoholausschank, Melderegistern oder Einberufungspraxen).

Überwachung kann man in diesem Sinn auch als Welt-Verstehen bezeichnen, nicht nur als Herrschaftsinstrument, um Gruppen aus- oder einzuschließen, sondern um ganz generell Welt zu erschließen und zu ordnen (vgl. auch Lyon 2001; Zurawski 2014). Datenbanken und Suchmaschinen, Algorithmen und Klassifikationen wollen

[5] *Doing privacy in everyday encounters with surveillance*: http://irissproject.eu/wp-content/uploads/2015/01/IRISS_DEL_4_2_Conduct_the_Observations_Interviews_2014_FINAL.pdf.

Übersichtlichkeit herstellen und Welt einteilen. Überwachung, Übersicht und Kontrolle sowie die entsprechenden Techniken fallen in dieser Betrachtung in eins zusammen.

3.2.3 Überwachung und Technik

Eine Erörterung von Überwachung ist kaum ohne Verweis auf eine bestimmte Technologie zu machen, die als Beispiel herhalten muss. Aber auch eine generelle Diskussion zu dem Thema kommt an dem Zusammenhang zur Technik/Technologie nicht vorbei. Wie bereits mehrfach erwähnt ist das, was Gary Marx (2002) als *new surveillance* bezeichnet, bestimmt durch die informationstechnischen Möglichkeiten, die Informatisierung und Computerisierung unserer Gesellschaften – Technologie steht also am Anfang dieser Entwicklung. *Big Data* und *social sorting* sind in der heute gekannten Weise nicht ohne Technologien möglich. Auch wenn Überwachung kein Phänomen ist, das an die Existenz von Technologien gebunden ist – und ich verwende hier absichtlich einen weiten Begriff von Technologien, der keine Unterscheidung zu Technik macht (Hengartner & Rolshoven 1998; vgl. auch Gaycken & Kurz 2008 im Hinblick auf Überwachungstechnologien) – so ist diese gegenwärtig ein zentraler Faktor in der Diskussion, in den Überwachungspraktiken und somit auch als vermittelnder Faktor in den sozialen Beziehungen, die möglicherweise durch Überwachung hergestellt werden.

Ich möchte hier nicht alle technischen Anwendungen, Technologien oder Geräte aufzählen und ihre Funktionsweise erklären. Vielmehr geht es darum auf ein paar wichtige Punkte hinzuweisen, die dieses Verhältnis kennzeichnen. Das gilt für eine wissenschaftliche Beschäftigung ebenso wie für die populären Debatten sowie die Vorstellungen von Anwendern für den Gebrauch von Technologien. Ein Grundgedanke, der dieses Verhältnis und viele Diskurse dominiert, ist jener der quasi allmächtigen Technologie, welche das Verhalten von Menschen und Gruppen beeinflusst oder gar bestimmt (vgl. u.a. Albrechtslund & Glud 2010). Die Kontextgebundenheit von Technologien und der respektiven Überwachung wird wenig bis gar nicht beachtet, wenn es um das Verhältnis von Technologie und Überwachung geht (vgl. u.a. Gottschalk-Mazouz 2008; Gaycken 2008; Timan 2013). Charakteristisch hierfür ist die Technik-deterministische Perspektive, die kaum berücksichtigt, dass mit Technik auch gehandelt werden muss, dass es durchaus verschiedene Verwendungen geben und Verhalten von vielen Faktoren abhängen kann.

Ein zweiter Aspekt, der das Verhältnis kennzeichnet, bezieht sich auf die Wünsche, was eine Technologie können soll und wie sie gesellschaftlich eingesetzt wird. Dabei handelt es sich immer um mittelbare Funktionen, die durch und mit Technologien erreicht werden sollen, selten aber um die Dinge, die sie technisch tatsächlich können. Kameras im öffentlichen Raum oder im Nahverkehr werden häufig mit der Begründung eingesetzt Kriminalität zu verhindern. Streng genommen können sie aber zunächst nur

Bilder aufnehmen oder ermöglichen eine Fernbeobachtung eines Raumes durch nicht anwesendes Kontrollpersonal. Ein gemeinsames Argument vieler als Überwachungstechnologien bezeichneter Systeme oder einzelner Artefakte ist, dass es sich dabei um Technologien für mehr Sicherheit handelt (vgl. u.a. Japp & Beck 2008; Harms, 2011; Pavone & Eposti 2012; Ammicht Quinn 2014). Das heißt, dass die Bedeutung und der symbolische Gehalt von Technologien mit dem eigentlichen Zweck verwechselt werden – was zugegebenermaßen nicht immer leicht auseinanderzuhalten ist. Ein Grund dafür ist sicherlich auch der Umstand, dass Technik eben nicht neutral ist, sondern Teil von Kultur und nicht ihr Gegenüber oder gar fremd dazu (Latour 1991; Rammert 2007, 2008, 2008a; Gottschalk-Mazouz 2008; Callon 2012; Hengartner 2012). So hat Klein für den deutschen Reisepass anhand der Diskurse gezeigt, welche Wünsche und Hoffnungen auf die Technik selbst übertragen werden. So wird im Zusammenhang mit dem biometrischen Reisepass von „Wunderwaffe" gesprochen, der eine „Revolution in der Sicherheitstechnik" im „Kampf gegen dem Terror" darstellt (vgl. Klein 2011, 87; auch Kurz 2008). Die Bundesregierung, so Klein, versprach sich von dem neuen ePass, dass er nicht nur fälschungssicher sei, sondern auch die Wirtschaft ankurbeln würde. Er war Teil eines „biometrischen Schutzwalles". Hier wird relativ deutlich ein Zusammenhang zwischen der eigentlichen Technik und darüber hinausgehenden Wünschen und möglichen Effekten gezogen.

Andere Arbeiten zum Verhältnis von Technologie und Überwachung zeigen, wie Technik als Projektionsfläche, wenn auch nicht immer offensichtlich, benutzt wird. Frois zeigt für die Videoüberwachung in Portugal (vgl. Frois 2013), dass der Wunsch „modern" zu sein einer der treibenden Gründe für die Anschaffung der Technik, jenseits der eigentlichen Funktionsweise oder der mittelbaren Möglichkeiten (Prävention, Überwachung), war. Ähnliche Ergebnisse findet man bei Purenne (2012) zu Pariser Polizisten und der Einführung von Überwachungstechnologie oder bei van Oijen & Bokhorst (2012) in einer Studie zu automatischer Nummernschilderkennung und der Arbeit der Polizei in den Niederlanden. Die Wechselwirkungen und auch die Effekte, die Technologien haben, sind andere als oftmals vor Einführung gemutmaßt. Letztlich wird an diesen wie auch an den folgenden Beispielen insbesondere deutlich, dass Artefakte (wenn man Technologien als solche begreift) politisches Potenzial besitzen. Bereits Winner (1980, 122) stellte fest, dass kaum eine technische Innovation auf der Bildfläche erscheint, die nicht das Versprechen einer Rettung der freien Gesellschaft mit sich bringt. Das gilt auch für die Technologien, die eine zivile Sicherheit versprechen. Technologie ist also stets nicht nur mit technischen Qualitäten versehen, sondern immer auch mit sozialen und politischen, die allerdings jenseits der Technik selbst liegen. Das liegt auch an dem bereits geäußerten Umstand, dass eine Bewertung von Technik anhand von Kriterien erfolgt, die nur mittelbar auf diese zurückzuführen sind. Die Beispiele Videoüberwachung auf der einen und biometrische Verfahren auf der anderen Seite bieten sich hier an, um die sich dort ergebende Lücke nachzuzeichnen.

Bei der Videoüberwachung, einem im Hinblick auf Überwachung sehr intensiv erforschten Feld (vgl. Klauser 2006; Zurawski 2007. 2011, 2014; zur politischen Bedeutung der Technik Hempel & Töpfer 2004; Hempel 2008 und 2009; Töpfer 2009; Armstrong & Norris 2010), liegt eines der Hauptargumente auf der kriminalpräventiven Wirkung oder der Abschreckung im öffentlichen Raum. Debatten und Diskurse über diese Technik knüpfen dort an. Dabei wird der mittelbare Zweck, Kriminalprävention, mit dem verwechselt, was die Technologie eigentlich macht: Filmen und das Gesehene gegebenenfalls speichern. Eine Sicherheits- und Überwachungstechnik wird sie nur im Kontext der Anwendung (sonst wäre die Filmbranche in toto auch dazuzuzählen). Wenn also als Ziel einer Kamerainstallation im öffentlichen Raum Sicherheit benannt wird, so kann das nur das mittelbare Interesse sein. Die Technologie verschafft vor allem denjenigen, die sie betreiben, eine bessere Übersicht ohne selbst vor Ort zu sein. Außerdem eine Zeit-unabhängige Betrachtung, wenn die Bilder aufgezeichnet werden. Die Sicherheit ergibt sich aus den auf die Kameras projizierten Wünschen und den Erzählungen, welche den Kontext bestimmen, ihn vorbereiten und die gefilmten Personen davon unterrichten, dass Kameras schauen, was gemacht wird und im Zweifelsfall ihr Verhalten Konsequenzen haben könnte. Sicherheit ist hier ein diskursiver Prozess, der hergestellt wird, sich aber nicht aus der Technik selbst ergibt, sondern aus dem Kontext von Anwendung, Machtverhältnissen, bürokratischen Erfordernissen und kommunizierten Erwartungen. Ähnliches kann für die mit dem Etikett Biometrie versehenen Technologien geschlossen werden (vgl. dazu auch Zurawski 2014).

Zu behaupten, dass biometrische Verfahren, wie sie sich gegenwärtig in der Entwicklung und im Einsatz befinden, mehr wollen, als bestimmte Muster zu erkennen (z.B. Irismuster, Fingerabdrücke oder standardisierte Verhaltensmuster), nämlich einem Menschen durch einen Blick in sein Inneres zu verstehen, wäre vielleicht gewagt, aber nicht unbedingt absurd. Aber der Anspruch der Technik ist es Identität festzustellen bzw. Identifizierungen an Kontrollpunkten durchzuführen. Das macht sie zu einer Sicherheitstechnik, denn die Annahme dahinter ist, dass auf diese Weise und mit einem Abgleich in Datenbanken, wo entsprechende Vermerke eingetragen sind, festgestellt werden kann, wer an welchem Ort kontrolliert wird, und ob diese Person Eintritt erhält oder andere Maßnahmen in Gang gesetzt werden müssen. Sicherheit ist also auch hier nur eine mittelbare Folge der Technologie, dann nämlich wenn der entsprechende Kontext geschaffen wird. Biometrie ist so gesehen mehr als nur die Tatsache, dass unsere Fingerabdrücke, unsere Iris, schlechthin unsere Körper mit bestimmten Methoden vermess- und kategorisierbar sind.

Angefangen bei den Gesetzen, die biometrische Verfahren in den Alltag einführen (vgl. Klein 2011), über die Personen, die die Kontrollen an den Grenzen durchführen, über die Unternehmen, die an den Technologien verdienen, bis hin zu den Körpern, die nun

vor allem als Träger von Merkmalen gesehen werden und schließlich den Praktiken der Vermessung und Überwachung selbst – sind dieses die Teile einer Praxis, die auch in uns hineinzuschauen versucht. Zentral geht es dabei um die Identität von Personen, technisch allerdings zunächst nur um das (Wieder-)Erkennen von Mustern des Auges, der Haut, des Blutes, der Stimme, des Gesichtes. Identität beschreibt wer jemand ist, geht dabei aber über eine Identifikation hinaus. Letztere bedeutet nur den Abgleich von Mustern – gespeicherten und erhobenen, d.h. kontrollierten. Vor allem geht es dabei um unsere Identität, um die Frage, wer jemand ist und wie sich dieser jemand einordnen lässt bzw. wie er oder sie wiederzuerkennen sind. Andererseits interessiert sich die Praxis der Biometrie ganz und gar nicht für die Identität einer Person und will auch nicht hineinschauen, sondern nutzt die Muster, um z.B. Ausländer ohne Papiere als Illegale zu klassifizieren, Asylansprüche zu prüfen oder die außereuropäischen Grenzen zu kontrollieren (vgl. van der Ploeg 1999, 2006). Das „Was“ und „Wie“ einer Identität spielt dabei keine Rolle, eher wird kontrolliert und vermessen, die Hintergründe von Flucht und Migration drohen vernachlässigt zu werden (vgl. Maguire et al. 2014). Biometrie dient hier der sozialen Aussortierung. In beiden Fällen – Aussortierung und Hineinschau – tritt das, was eine Identität in ihrer Komplexität ausmacht, in den Hintergrund. Identität ist innerhalb der biometrischen Praxis eine verfügbare Größe der Identifizierungsmaßnahmen. Um zu identifizieren, wird Identität einerseits auf eine Kontrollfläche, ein Interface projiziert und von dem Menschen als Subjekt entkoppelt. Gleichzeitig gibt es eine gegenläufige Tendenz, über die unsere biometrischen Merkmale immer enger an Identität gekoppelt werden. Damit wird der Anschein erweckt, dass es möglich ist, unsere Identität in ihrem sehr eigenen (und engen) Sinn unzweideutig festgelegen zu können. Das jedoch wirft die Frage auf, welche Art von Identität damit gemeint sein könnte, zu welchem Zweck und mit welchem Ziel das passiert und was von uns übrig bleibt, wenn wir in Bilder, Merkmale und digitale Zahlenkolonnen zerlegt (und neu zusammengesetzt) werden. Die Politik der Identität oder Identitätspolitik spielt bei der Einführung und Durchsetzung von Biometrie als Verfahren und Praxis eine enorm wichtige Rolle, für die Beantwortung der Frage, was als Identität wofür gebraucht wird und wieso diese mit Biometrie überprüft werden muss (vgl. auch Neyland 2009; Klein 2011). Die Einzigartigkeit des Individuums, so scheint es, wird ersetzt durch die Einzigartigkeit seiner extrahierten Einzelteile und Merkmale. Aus Identität wird ein Muster, eine Strategie der Identifikation.

Ein alleiniger Fokus auf Mustererkennungstechnologien greift analytisch zu kurz und erscheint oft nicht mehr als ein ängstlicher Warnruf *„Schaut her, was die machen – die können meine Muster erkennen“*. Muster zu erkennen und einzuordnen ist jedoch die Grundvoraussetzung für menschliches Verhalten und soziales Zusammenspiel. Erst der Kontext entscheidet, ob es sich dabei um ein kontrollierendes, überwachendes Verhalten handelt, und ob es dabei um die gezielte Manipulation und Steuerung von Menschen (sowie deren möglichen Ausschluss) oder doch deren Fürsorge handelt – und ob davon

grundlegende Freiheiten und Rechte betroffen sind. Außerdem würde eine gezielte Analyse des Kontextes auch die Handlungen und eventuellen Neuinterpretationen der Handelnden mit einbeziehen, womit die Dynamik eine adäquate Aufmerksamkeit erfahren würde. Da Technik nicht ohne weiteres einfach nur funktioniert, sondern auch aufgeladen mit Wünschen und Hoffnungen ist, soll am Beispiel der biometrischen Identitätserkennung erläutert werden. Dort wird versucht mit Hilfe der Technik zu verstehen, obwohl es tatsächlich über einen Musterabgleich nicht hinaus reicht. Leider liegt hierin die fatale Qualität aller Anstrengungen menschliche Muster und Verhaltensweisen zu messen und zu speichern. Der Wunsch zu verstehen schafft den Kontext für die Technik und ihre Konsequenzen – ohne diesen Wunsch wäre Biometrie nicht das, worüber wir heute diskutieren und wovor Kurz in ihrem Artikel über die Möglichkeiten und Konsequenzen vernetzter Biometrie warnt.

Damit Mechanismen und Praktiken der Ordnung wie *Identität* funktionieren und unzweifelhaft ablaufen können, muss eine Identität verifiziert werden. Während Identität wechselhaft, konstruiert, aushandelbar, falsch, vorgespielt, sozial verankert, Kontext-gebunden sein kann, ist Identifizierung klar und eindeutig. Die Frage, die durch Identifikationen immer beantwortet werden soll, ist „wer ist es?“. Die Antwortmöglichkeiten sind vielfältig, und sie reichen von genealogischen Zuordnungen (Sohn, Tochter von XY), über soziale Beziehungen bis hin zu persönlichen, intimen, biologischen Kennzeichen oder dem Namen, der wiederum eine legal-soziale Größe darstellt (vgl. Marx 2006, 94f). Welche Art der Identität benutzt werden kann oder erwünscht ist, ist von der Situation abhängig. Biometrische Verfahren lassen allerdings nur eine Art von Merkmalen zu, was den Körper und damit Personen zu einer Ansammlung von Informationen macht (vgl. Lyon 2007, 112)

Solche „falschen“ oder unzureichenden Übertragungen von Wünschen auf die tatsächlichen Leistungen bzw. die späteren Einsatzziele können für beliebige Technologien gezeigt werden. Was die Überwachungstechnologien betrifft, kann man im wesentlichen drei Kategorien – Sehen, Muster erkennen, Statistik (und eine Unterkategorie: bürokratische Identifikation) unterscheiden, mit denen sich so ziemlich alle Verfahren in Bezug auf ihre technischen Möglichkeiten und die sie umgebenden Sicherheitsdiskurse beschreiben lassen.

Technik/ Funktionsweise	Anwendung	Ziel	Einsatz
sehen, hören, aufzeichnen	Kamera, tracking, Lauschangriff, Onlinedurchsuchung	Prävention, Übersicht, Spionage, Detektion (Kontrolle)	Raum, Person
Muster erkennen	Biometrie (DNA, Iris, Fingerabdruck etc.)	Suche, Kontrolle	Person, Massenüberwachung
Zusammenhänge, Gewohnheiten, statistische Übersicht	Datenbanken	Suche, Analyse, Steuerung, Management	unpersönlich, Massenüberwachung, Person als Data double
Bürokratische Identifikation	Pässe, Ausweise	Kontrolle, Management, Prävention	Person, Massenüberwachung

Abbildung 2: Kategorien der Überwachungstechniken (eigene Darstellung)

Die Unterkategorie der Pässe gehört zu den Datenbanken, überschneidet sich je nach Kontext und Form der Identitätstechnik mit den anderen Kategorien. Zwischen den einzelnen Kategorien gibt es jeweils Überschneidungen bzw. die entsprechenden Technologien werden ergänzend und in Kombination angewendet. Zu unterscheiden wäre bei den im Einzelnen verwandten Technologien noch, ob es sich dabei um eine Massenüberwachung handelt, oder um Maßnahmen, die eher auf einzelne Personen gerichtet sind (vgl. auch Gottschalk-Mazouz 2008, und sein Modell einer ganzheitlichen Überwachung). Zusammenhänge von Überwachung und Technologie im Hinblick auf Sicherheit lassen sich mit Hilfe dieser Matrix veranschaulichen. Sicherheit ist ein Konstrukt, das auf Diskursen aufbaut, die aus Aspekten von Überwachung und den Übertragungen technischer Funktionsweisen zusammengesetzt sind. Der Begriff Sicherheitstechnologie beschreibt so eher den Kontext der Nutzung als die technische Innovation selbst – womit allein schon die Neutralität von Technologie in Frage gestellt würde. Eine hier sinnvolle Perspektive auf Technik und Technikkultur wäre eine ökologische, mit der das Geflecht aus Beziehungen und Bedeutungen in den Mittelpunkt rückt, und nicht so sehr kausale Abfolgen oder Hierarchien (vgl. u.a. Vannini 2009, 73ff.).

Die Techniken und Technologien zur Kontrolle menschlicher Aktivitäten sind vielfältig, hinsichtlich der zur Anwendung kommenden technischen Artefakte, ihrer Strategien und schließlich bezogen auf die Felder bzw. die gesellschaftlichen Zusammenhänge, innerhalb derer kontrolliert wird. Zudem müssen die vorkommenden Formen der Kontrolle unterschiedlich beschrieben und bewertet werden. Kontrolle soll hier von Überwachung unterschieden werden, in dem Sinn, dass Kontrolle zunächst nicht auf die Steuerung, die Erziehung oder Disziplinierung von Menschen ausgerichtet ist. Kontrolle beschreibt das Sammeln und Protokollieren von Daten und menschlicher Aktivität einerseits, sowie die spätere zielgerichtete Auswertung, Überprüfung und Verwendung dieser Daten und Handlungen (vgl. Kammerer 2009, der die ursprüngliche Bedeutung des Wortes im französischen mit *Rechnungsprüfung* angibt). Hinsichtlich der Verwendung von Daten und Einträgen könnte man wieder von Steuerung sprechen, zumindest lägen hierin Möglichkeiten Prozesse zu beeinflussen oder in diese gestaltend einzugreifen. An dieser Stelle beginnen sich Kontrolle und Überwachung zu überlappen. Aus dem Sammeln und Vorhalten von Daten wird durch zielgerichtete und routinierte Strategien eine Überwachung von Einzelnen oder ganzen Gruppen, bzw. von Kategorien von Individuen, die in klassifizierten Gruppen immer wieder neu geordnet werden (vgl. Bogard 2006; Lyon 2008). Dabei zielt Überwachung nicht nur auf die strategische (und weitgehend anonymisierte) Einteilung von Gruppen von Menschen, z.B. zum Zwecke der Konsumforschung, des Freizeitverhaltens, der allgemeinen Mobilität u.a., sondern darauf, gezielt über diese Daten an das Verhalten einzelner zu gelangen, diese einem Verdacht auszusetzen (der auch falsifiziert werden kann) und eventuell Rechte und Pflichten anhand der gewonnen Daten abzuleiten. Es ist nicht immer eindeutig, ob es sich im jeweiligen Fall um Kontrolle oder um Überwachung handelt. Kontrolltechnologien stellen somit die strategischen, herrschaftlichen, in vielen Fällen auch die prothetischen Voraussetzungen für verschiedene Bereiche von Überwachung dar.

Der Begriff der Kontrolltechnologien betrifft zwar pauschal alle Aspekte sozialen und kulturellen Lebens, dennoch muss eine Unterscheidung hinsichtlich der möglichen Bedeutungen und letztlich der theoretischen Anwendung gemacht werden. Grundsätzlich sollen Technologien zunächst die größeren systemischen Zusammenhänge bezeichnen, in denen einzelne Artefakte als Bestandteile einen Platz haben, z.B. das System Pass, bestehend aus Gesetzen, Papieren, Chips, Datenbanken, Politik und Auswahlkriterien/Klassifikationen. Darin eingebettet sind Kontrolltechnologien im Sinne Artefakt-vermittelter Techniken, mit denen Kontrollpraktiken vollzogen werden bzw. die diese bereits implizieren, z.B. Messeinheiten oder Ausweise zum Identitätsabgleich. Man kann hier auch von Anwendungsfeldern sprechen, in denen Kontrolltechnologien im Sinne zweckrationaler und systemischer Zusammenhänge vorkommen, und in denen diese als kulturelle Praktiken empirisch untersucht werden können. Dazu gehören u.a. *Konsum(kontroll)technologien*, zum Zwecke des Marketing

und der Logistik beim Warenkonsum; die *hoheitliche Kontrolle* durch Pässe an Grenzen, zur erkennungsdienstlichen Behandlung durch die Polizei u.v.a.; *Identifizierungstechnologien*, mit denen Grenzübertritte möglich gemacht werden, – Einlasskontrollen, Berechtigungskontrollen usw.; oder *Umwelt(kontroll)ltechnologien*, mit denen z.B. Wetterdaten oder die Wasserwerte eines Flusses gemessen werden. Damit Kontrolle in diesen Anwendungsfeldern überhaupt ausgeübt werden kann, gehen diesen technologischen Systemen und Artefakt-induzierten Technologien notwendigerweise Technologien im Sinne eines zweckrationalen Handelns voraus. Diese sind notwendig, um über ein Artefakt ein bestimmtes Ziel zu erreichen. Ein Ausweis ohne entsprechende Klassifikationen, Einteilungen oder Gesetze ist ein Stück Plastik, aber keine Technologie im hier skizzierten Sinn. Der Begriff Technologie impliziert immer auch Fertigkeiten, sinnhafte Systeme der Klassifikation oder logische Handlungsanweisungen, die zielgerichtet sein sollen. Darunter sollen auch die im Anschluss an Foucault als Selbsttechniken/-technologien bezeichneten Praktiken und erlernten Fähigkeiten gefasst werden, auch wenn diese nicht auf andere gerichtet sind. Ein banales Beispiel dafür wäre z.B. das Trainieren des Körpers, um in einer Leistungsgesellschaft mithalten zu können. Aber auch das Trainieren von Handlungsabläufen, die möglicherweise zur besseren Integration in eine Gesellschaft beitragen können gehören dazu: Weiterbildung, Nutzung sozialer Medien, Zurschaustellung des Selbst in bestimmter Weise. Diese können, müssen aber nicht notwendigerweise, technisch vermittelt sein. Hinsichtlich der Kontrolltechnologien würden darunter auch solche Artefakt-vermittelten Technologien fallen, die von einem Subjekt auf sich selbst bezogen angewendet werden – etwa zur Kontrolle, selbstständigen Einteilung oder Bewertung des Selbst aus und zur Eigenermächtigung.

Dass in der Praxis diese hier gemachten Begriffsunterschiede nur selten in der reinen Form und Definition vorkommen, ergibt sich aus den Abhängigkeiten und Konsequenzen der Technologien. Hinsichtlich der Kontrolle sind die Klassifikationen – also auf Wissen basierende Handlungsanweisungen – Grundlage für Artefakte, über die eine z.B. eine Identifikation entlang der vorgegebenen Klassifikationen vorgenommen wird. Anderseits, induzieren auch Artefakte bestimmte neue Handlungsanweisungen oder machen diese erst möglich, so dass der systemische Charakter von Kontrolltechnologien in diesem Fall hervorgehoben werden muss.

Forschungspraktisch bedeutet das, dass man drei Ebenen definieren kann, mit denen sich die unterschiedlichen Aspekte solcher Technologien im Einzelnen und ihrer Probleme und der damit verbundenen Diskurse/Narrative im Allgemeinen nachspüren lassen. Dabei werden Ebenen der Abstraktion und der Operationalierung für die Forschung unterschieden: von den Theorien (Makro), über die einzelnen Merkmale sowie deren Folgen und Bedingungen (Meso), bis hin den konkreten Praktiken durch die Nutzer

- Auf einer *Makroebene* wäre zu diskutieren, was Kontrolle analytisch umfassen würde (Definition) und wie Kontrolle über Technologien vermittelt und in diese eingeschrieben – im Sinne des Sammelns von Daten aller Arten – funktioniert. Damit verbunden ist auch die Frage, wann eine Kontrolltechnologie eine solche ist, was sie ausmacht und welche Formen technischer Artefakte dazu gehören können.
  –> Theorie, Konzeption

- Auf der *mittleren Ebene* könnten die mit Kontrolltechnologien verbundenen Diskurse der Macht, ihr Überwachungspotenzial sowie insbesondere die sozialen, politischen und kulturellen Konsequenzen von Klassifizierung, Normierung oder Ausschluss diskutiert werden. Hier könnte man auch die Handlungsanweisungen, die Kategorien, Klassifikationen und notwendigen Logiken untersuchen, die notwendige Voraussetzungen sowohl für die Aspekte der Mikro- und Makroebene sind.
  –> Operationalisierung von Forschung sowie Fokus auf mögliche Implikationen von Technologie; kontextuelle Rahmung für Forschung.

- Daran anschließend wäre es möglich auf einer *Mikroebene* sich mit einer der oben aufgeführten Kontrolltechnologien im Detail zu beschäftigen. Dabei müssten dann nicht nur die spezifischen technischen Besonderheiten für den einen Bereich im Mittelpunkt stehen – vielmehr würde eine Forschung auf dieser Mikroebene einen Blick von unten, durch die sozialen und kulturellen Praxen ihrer Benutzer bedeuten, in welche eine der Kontrolltechnologien eingebettet ist oder in der sie vorrangig vorkommt. Eine kulturwissenschaftliche Technikforschung bedeutet, das zentrale Augenmerk auf eben diese Mikroebene zu legen und die Konsequenzen dieser Mikroebene für die anderen beiden nachzuzeichnen – ausgehend von der Bedeutung einer Kontrolltechnologie innerhalb einer (oder mehrerer) spezifischen sozialen oder kulturellen Praxis.
  –> Empirie, insbesondere ethnographische Methoden der Untersuchung von Technik und dem Umgang mit Technik.

So könnten bei Konsum(kontroll)technologien beispielsweise Praktiken gemeint sein (Artefakt vermittelt oder nicht), die den persönlichen Verbrauch an etwas kontrollieren, z.B. Drogen oder Energiegüter mit dem Ziel einer Kontrolle eigenen Verhaltens um Veränderungen zu initiieren oder abzubilden. Ebenso können aber Technologien gemeint sein, mit denen der Warenverbrauch von Personen oder Gruppen von Personen die vielfältigen Zusammenhänge des Konsums kontrolliert, protokolliert und in neuen Verbindungen und Verknüpfungen weiter zu anderen Zwecken verwendet werden. Dabei kann es sich auch um solche Techniken/Technologien handeln, die bildlich gemeint eingebettet in die Güter und Dienstleistungen sind, die ohne ein explizites Technikhandeln des Menschen aktiv sind oder werden und gegebenenfalls auch mit anderen Techniken/Technologien kommunizieren *(bekannt unter dem Stichwort ubiquitious computing)*. Dies alles könnte man auf der Makroebene der Analyse

verorten. Dass sich die anvisierten Technologien damit mitten in der Diskussion zu Überwachung, Kontrolle, Datenschutz und den damit verbundenen Theorien, Diskursen und Erklärungsansätzen befinden, wäre analytisch wichtig für die Mesoebene. Dazu gehören auch die Bedingungen und operationalen Kategorien dieser Diskurse. Auf der Mikroebene stehen dann die konkreten Artefakte im Zentrum, über die ein Zugang zu den Kontrolltechnologien innerhalb kultureller Praktiken empirisch geschaffen wird. Die drei Ebenen beschreiben Zugänge zu dem Themenkomplex, die nie ausschließlich gesehen werden sollen, sondern über vielfältige Verbindungen aufeinander wirken – sowohl theoretisch, als auch in einer praktischen Forschung.

Für eine kulturwissenschaftliche Forschung halte ich dabei die Konzentration auf die Praktiken für einen zentralen Aspekt, innerhalb derer die durch die Techniken evozierten Diskurse, jene Technologien ermöglichen, diese angewandt, mit Bedeutung oder eben als Teil der Handlung in die sozialen und kulturellen Praktiken eingebettet werden.

Die beschriebenen Kategorien stellen keine diskreten Bereiche dar, sondern geben viel eher Schwerpunkte an und situieren eine Technologie innerhalb eines Feldes, z.B. Konsum oder Grenzregime. Die Überlappungen herauszuarbeiten wäre ebenfalls Aufgabe einer Mikroebene, wie es z.B. für die Kundenkarten im Bereich der Konsum(kontroll)technologien im weiteren Verlauf gemacht wurde.

3.2.4 Überwachung als soziale Praxis und soziales Handeln

Wie zu Beginn bereits festgestellt wurde, handelt es sich bei Überwachung vornehmlich um eine Handlung. Das bedeutet jedoch, dass es auch Akteure geben muss, die überwachen. Und somit gibt es auch Praktiken, aus denen heraus sich etwas bildet, das analytisch als Überwachung gefasst werden kann. Bisher allerdings war davon eher weniger die Rede. Und das gilt auch für die theoretischen Zugänge zum Thema, die weiter oben vorgestellt worden sind. Darin liegt der Fokus in der Regel auf der Überwachung durch Institutionen, was die oftmals auch beteiligten Menschen weitestgehend unberücksichtigt lässt. Variationen oder Ergänzungen zu den bestimmenden Ansätzen ändern diesen Fokus im Grundsatz nicht. Der Vorschlag für eine andere Sichtweise zu Überwachung könnte daher hilfreich sein, um diese Dimension von Überwachung auch zu begreifen und ihr ein theoretisches Gesicht zu geben. Monahan spricht davon Überwachung als kulturelle (und soziale) Praxis zu begreifen, da Akteure in ihrem Handeln ständig, gezielt oder auch unreflektiert auf kulturelles Wissen zurückgreifen (vgl. Monahan 2011; Zurawski 2011und 2014). Ähnlich wie alle anderen Technologien, sind auch Überwachungstechniken verhandelbare Bestandteile von Kultur und somit Teil kultureller und auch sozialer Praktiken, die entweder darüber vermittelt werden oder konstitutiv für diese sind. Deshalb wird nun ein Blick auf Praktiken der

Überwachung, die Akteure und die durch Überwachung konstituierten sozialen Beziehungen geworfen.

Überwachung als soziale oder kulturelle Praxis zu begreifen, wie es zunehmend auch durch den Einfluss ethnographischer Forschung und kulturwissenschaftlicher Ansätze in diesem Bereich getan wird, bedeutet daher folgendes:

1. Überwachung als Ausdruck von Handlungen zu verstehen – und damit einen Blick auf die Akteure und ihre sozialen Beziehungen in der Ausübung dieser Praktiken zu werfen;

2. zu verstehen, dass soziales und kulturell bedingtes Handeln Überwachung hervorbringt, die als solche in der Praxis nicht so benannt wird, analytisch aber alle Merkmale dafür erfüllt; und

3. dass dieses Handeln, den Umgang mit Technik (wo vorhanden) mit einschließt – Technik also nicht eine Ergänzung dieser Praktiken ist, sondern diese begründen kann, zumindest aber mit diesen so verwoben ist, dass man von Technik als sozialem und kulturellem Gut sprechen kann (Hengartner 1998; Gaycken 2008; Rammert 2007, 2008, 2008a; Heßler 2012; Recki 2013; Häußling 2014).

Die Bedeutung einer Perspektive, die Überwachung in ihrer kulturellen und sozialen Verankerung betrachtet (vgl. Zurawski 2011) erschließt sich zunächst vor allem, wenn wir die bisherigen Perspektiven hinsichtlich ihrer Potenziale, Erklärungshorizonte und Grenzen betrachten. Forschung zu Überwachung bedeutet sehr häufig eine Konzentration auf die beobachtbare und an Artefakten ausgerichtete technische Dimension von Überwachung, wie auch das Kapitel zu den Zusammenhängen zwischen Überwachung und Technik deutlich gemacht hat. Hier manifestiert sich Überwachung jenseits eines abstrakten Modells über die Strukturen, in den Technologien, die so häufig als Objekt vieler Forschung so etwas wie das populäre Gesicht der unterschiedlichen akademischen, populären und politischen Diskurse darstellen: Videokameras, biometrische Pässe, Iris-Scanner, DNA-Analysen, der klassische Fingerabdruck oder das Internet sind die üblicherweise genannten. Als weitere kann man Technologien wie MRTs zur (erhofften) Erkennung von Denkmustern, digitale Bildaufzeichnungen, Satelliten oder die somatische Überwachung von Körperfunktionen in hochmodernen Kampfanzügen von Soldaten sowie Körperimplantate nennen (vgl. Monahan 2007; Monahan & Fischer 2010). Der empirische Zugang zu Überwachung hat seinen Ausgangspunkt sehr häufig in der Bewertung solcher Technologien bzw. der einzelnen technischen Artefakte hinsichtlich ihrer sozialen oder ethischen Konsequenzen, ihrer politischen sowie legalen Rechtmäßigkeit. Ein an der technischen Dimension ausgerichteter Ansatz nutzt Technik als Einstieg, um über das Artefakt selbst hinausgehende Beziehungen zu erkunden. Dabei besteht die Gefahr, Technik als bloßes Objekt zu

nutzen, ohne die Artefakte in ihren Wirkungen und Bedeutungen selbst zu unterscheiden. Rechtliche oder politische Bewertungen würden dann vorgenommen ohne mögliche Bedeutungs- oder Zuschreibungsunterschiede zu thematisieren. Die technische Dimension darf nicht dazu verleiten, lediglich verschiedene Techniken nach dem einen oder anderen theoretischen Muster abzuhandeln oder gar schon als Ausdruck von Überwachung an sich zu betrachten. Vielmehr soll mit dem Fokus auf Technik, ihrer Rolle als einem besonderen Element von Überwachung Rechnung getragen werden. So gehören dazu auch Bereiche, die üblicherweise nicht sofort als Technik erkannt oder als solche bezeichnet werden, dieses aber durchaus sind, wie z.B. Architektur oder Stadtplanung. Auch bürokratische Verfahren kann man dazu zählen, insbesondere dann, wenn Sie über Software vermittelt bzw. ausgeübt werden. Technik als Einstieg zu wählen, bedeutet Überwachung über den Weg materieller oder immaterieller Phänomene zu betrachten. Andere Dimensionen, wie z.B. eine soziale oder rechtliche, würden in diesem Fall der Technik nachgeordnet sein. Letztere sind weitere Dimensionen für eine Betrachtung, nicht zuletzt, da es sich um Menschen und Gruppen von Personen handelt, die unter Überwachung, Kontrolle und Überprüfung stehen, die überwachen und entscheiden, die ausgegrenzt oder eingeschlossen, diskriminiert oder bevorzugt werden, die Hilfe erfahren oder vergessen werden.

Die rechtliche Dimension von Überwachung eröffnet einen Zugang, in dem Maßnahmen oder Regelungen als Teil einer normativen Ordnung begriffen werden können, sowie zu den sich möglicherweise ergebenden Störungen, Abweichungen oder Herausforderungen des Rechtssystems. Schaut man auf die sozialen Dimensionen von Überwachung, dann sind damit die Formen der Vermittlung oder der Kontrolle sozialer Normen gemeint. Diesbezüglich würde man sich dann damit beschäftigen zu schauen, inwiefern die Beziehungen von Individuen in einer Gesellschaft davon betroffen sind und wie Vergesellschaftung unter welchen Bedingungen auch immer sich verändert oder überhaupt möglich ist. Eine Perspektive, die Überwachung in ihrer sozialen Dimension untersucht, schaut nach den Formen und Möglichkeiten gesellschaftlicher Teilhabe und genereller gesellschaftlicher Strukturen unter den Bedingungen von Überwachung – ohne das letztere bis jetzt überhaupt genauer definiert wurde.

Es ist offensichtlich, dass keine der hier kurz skizzierten Dimensionen pur und ausschließlich das eine oder andere Phänomen von Überwachung ausmacht. Wie bei vielem bieten sich durch die unterschiedlichen Dimensionen unterschiedliche Bewertungsansätze, werden öffentliche Debatten und akademische Diskurse von ihnen bestimmt. Forschung zum Thema kann immer mehrere dieser Blickwinkel einschließen, mit jeweils unterschiedlich gesetzten Schwerpunkten. Es ist allerdings wichtig zu verstehen, dass sich Überwachung nicht allein aus dem Vorhandensein einer Kamera erklären lässt oder ein, wenn auch präferiertes, theoretisches Modell über alle Phänomene gleichermaßen gezogen werden kann. Überwachung ist mehrdimensional

und bietet durch die Mehrdimensionalität des Phänomens zahlreiche Ansatzpunkte zur theoretischen und empirischen Forschung.

Allerdings fehlt bei all den aufgezählten Dimensionen jene, die beschreibt und analysiert wie sich Überwachung praktisch manifestiert und was das für die Erforschung des Phänomens bedeutet.

Es gibt zwar eine Übereinkunft darüber, was das Phänomen ausmacht, allerdings wenig Erklärendes dazu wie und wo Überwachung passiert und unter welchen Beschreibungen und mit welchen kulturellen Hintergründen diese rationalisiert werden. Sie ist zunächst einmal da – symbolisiert oder manifestiert in Techniken, Gesetzen, sozialen Verwerfungen oder theoretischen Modellen. Doch es bieten sich durchaus auch alternative Sichtweisen bekannter Konstellationen an, die darauf verweisen, dass eine kulturelle Praxis wichtig für die Analyse von Überwachung ist. Das bedeutet allerdings nicht, dass jede Überwachung mit dem Verweis auf eine wie auch immer ausgestaltete kulturelle Praxis oder eigensinnige Interpretation durch die Akteure gerechtfertigt werden kann.

Das Panopticon ist ein Gefängnis, eine Architektur-Technik, in der das Verhältnis von Wärter und Gefangenem eingeschrieben ist. Wie aber sieht der Alltag der Gefangenen aus, wie der der Wärter? Welche Praktiken bestimmen ihr Verhältnis zu der Architektur? Und inwieweit bestimmt die Technik ihr Handeln? Es ist unwahrscheinlich, dass die einseitige Beobachtung des Gefangenen durch den Wärter das Einzige ist, was darin stattfindet und niemand arbeitet, speist, schläft oder – im Falle der Wärter – nach Hause geht oder gar auf der Wache einschläft. Das galt bei der Konzipierung des Panopticons durch Bentham und trifft auf heutige Formen der Überwachung gleichermaßen zu. Denn, Überwachung hat durchaus auch eine praktische Dimension. Da sie letztlich irgendwo und irgendwie „passiert“, muss sie in Handlungen eingebettet sein und wird letztlich durch diese überhaupt erst erfahrbar. Überwachen ist eine Tätigkeit. Es gibt fast immer einen Punkt, an dem innerhalb einer Abfolge von Entscheidungen und rechtlichen Rahmenbedingungen, theoretischen Annahmen und technologischen Voraussetzungen gehandelt wird. Dort kommen Menschen vermittelt über Technologien oder durch Gesetze und Vorschriften in Kontakt, und es können sich generelle, allgemeinere Praxen von Überwachung und Kontrolle überhaupt erst herausbilden. An diesen Stellen kann man Überwachung *arbeiten* sehen – auch wenn sie oft dann nicht so heißt oder auf den ersten Blick als solche zu erkennen ist. In vielen Fällen werden zunächst einmal Vorschriften umgesetzt, wobei Menschen inneren und äußeren Zwängen ausgesetzt sind. Diese Vorschriften sind nicht per se auf die Überwachung anderer angelegt, können aber in der Konsequenz als solche empfunden werden. Auch sagen Vorschriften wenig darüber aus, wie z.B. Wachpersonal die ihnen übertragene Aufgabe konkret auszuführen hat, welche eigenen Vorstellungen ihre tägliche Arbeit beeinflussen und wie sich darauf neue Praxen der Überwachung oder auch des Widerstandes oder Neu-Interpretation herausbilden

können. In Bezug auf die mittlerweile zur Ikone gewordenen Videokameras – gleich ob im öffentlichen Raum, in U-Bahnen oder Shopping Malls – kann man nicht nur wegen der Technik selbst von einer Überwachungsmaßnahme sprechen. Vielmehr müssen bei Untersuchungen und Bewertungen auch die Menschen und ihre Praktiken in Betracht gezogen werden, die aus einer installierten Kamera eine Überwachungsmaßnahme werden lassen. Norris & Armstrong (1999) und McCahill (2002) haben mit ihren Studien zu den Überwachern und den inneren Strukturen von Kontrollräumen einen wichtigen Betrag geleistet, an den sich hier auch über die Kameras hinaus anschließen ließe. Aufzeichnungen müssen angeschaut werden, Verdächtigungen und die ihnen zugrunde liegenden Kategorien der Bewertung sind keine ontologischen Tatsachen, sondern sozial konstruiert. Der Arbeitsalltag ist oft langweilig und von den üblichen Strukturen abhängiger Arbeitsverhältnisse sowohl mit den Chefs als auch untereinander geprägt. Und manchmal lässt auch die konkrete Praxis nicht vermuten, dass es sich um mehr handeln sollte, als um einen Wachgang, der eine Form der Überwachung darstellt, aber in den üblichen Theorien eher blass bleibt. Sicherheitskräfte können des nachts um leere Grundstücke herumlaufen, ohne dass ihre Kontrolltätigkeit einen Einfluss auf andere Menschen hat, noch dass sich ihre Praxen konkret in einen größeren Zusammenhang „Überwachungsstaat“ stellen ließen – ohne von der Gesellschaft als Überwachungsstaat per se sprechen zu müssen. Überwachung in diesem Sinn ist nicht immer prickelnd, in seinen konkreten Formen nicht immer gefährlich und trägt nicht unbedingt den gesamten „Überwachungsstaat“ mit sich herum. Auch sind viele dieser Maßnahmen nicht geplant im Hinblick darauf, Teile eines größeren Zusammenhanges in einer „Überwachungsgesellschaft“ zu sein. Sie spiegeln Trends wider, sind aber Einzelentscheidungen, die nur in der Summe und nur von außen ein von innen nicht erkennbares Bild größerer Überwachungs- und Kontrollzusammenhänge ergeben. Viele der Maßnahmen, Angebote, Verfahren oder Techniken, die als Überwachung bezeichnet werden, sind aus den Notwendigkeiten wirtschaftlicher Gewinnmaximierung oder bürokratischer Erfordernisse heraus entstanden – kein böswilliger Staat hat sie sich ausgedacht um dem Ideal des Big Brother oder eines allumfassenden Panopticon nachzueifern. Und genau deshalb werden manche dieser Maßnahmen nicht als Überwachung oder Kontrolle wahrgenommen. So kann man mit Kundenkarten nämlich tatsächlich einkaufen gehen, was bedeutet, dass die damit verbundene Praxis das Einkaufen und nicht der Datenschutz bzw. das Ausspionieren der Kunden ist. Aus demselben Grund sind die Kunden aber auch so „fahrlässig“ und lassen sich ins Portemonnaie und die Einkaufstasche sowie ihre Lebensgewohnheiten schauen (vgl. Zurawski 2011a).

Der Blick auf die praktische Dimension von Überwachung ermöglicht nicht nur hier eine Analyse der offenen, verdeckten, beabsichtigten oder kollateralen Formen von Überwachung und Kontrolle. Oft sind Teile davon in diesen Praktiken erkennbar, unter Umständen in sie eingeschrieben oder werden über sie vermittelt.

Ganz generell gehört dazu, die Perspektive auf die praktischen Aspekte von Überwachung/Kontrolle zu lenken, und diese in ihren jeweiligen Formen zu beschreiben. Hiermit ist vor allem die Frage nach den Eigenarten und eigenständigen Logiken gemeint, die verschiedene Praktiken innerhalb verschiedener Anwendungsgebiete haben, z.B. bei der Polizei im Gegensatz zum Kaufhaus, in einem Ministerium im Unterschied zu einem Bordell. Was macht eine konkrete Praxis so speziell und welche Bedeutung kommt ihr in einem größeren gesellschaftlichen Rahmen zu? Nur über diese grundsätzlichen Fragen kann erörtert werden, welche theoretischen Schlüsse man aus den Praktiken für eine Theorie von Überwachung ableiten kann. Das Überwachung kleinteiliger ist, als die Verwendung des Begriffes oft vermuten lässt, dürfte mittlerweile keine großen Diskussionen hervorrufen. Zu klären ist dann anhand von empirischem Material, welche Aspekte einer „Überwachungs-/Kontrollgesellschaft“ über eine spezielle Praktik vermittelt werden und wie diese eventuell in diese eingeschrieben sind bzw. von dieser als Teilaspekt repräsentiert werden. Die Analyse von Praktiken bietet die Chance die Bedeutung des Subjektes innerhalb von Zusammenhängen zu untersuchen, in denen es in der Regel als passives Objekt verharren muss bzw. als Spielball undurchschaubarer, „dunkler“ Mächte. Ist es eigenständig oder doch nur ein gezwungener Teil eines Systems, eines Handlungszwanges, den es selbst nicht durchdringen kann? Wenn es tatsächlich eigenständig ist, drängt sich die Frage nach den möglichen Widerstandspotenzialen gegen Überwachungspraktiken auf. Sind diese vorhanden? Werden sie genutzt? Und was passiert mit einer Maßnahme, wenn die Idee durch Handlungen konterkariert wird? Letztlich gilt es immer auch zu klären, worauf sich eine Überwachungspraxis bezieht, ob es klare Vorgaben und Ziele gibt oder ob es sich um eine selbst-generierende Praktik handelt, in der nur durch die Tätigkeiten selbst ein Ziel erkennbar werden kann. In Bezug auf Technologie ist vom *function creep* die Rede, wenn neben den ursprünglichen Einsatzgebieten sich neue allein dadurch ergeben, dass sich ein Einsatz lohnt und möglich ist. Die Verwendung von RFID ist ein Beispiel dafür, wie aus einer Technologie ursprünglich zur Warenverfolgung zu logistischen Zwecken, eine Überwachungs- und Kontrolltechnologie mit Anwendungsgebieten für Menschen bzw. zur möglichen Steuerung von Menschengruppen, Menschenströmen und damit auch wieder einzelner Individuen geworden ist (vgl. Rosol 2007).

Die Perspektive auf die Praktiken von Überwachung (Kontrolle, Überprüfung) bzw. solchen Praktiken, die an Überwachungs- und Kontrollregime anschlussfähig sind, ist deshalb so wichtig, weil hierdurch die tatsächlichen Aushandlungsprozesse deutlich werden können, die es braucht, um Überwachung im Großen zu analysieren. So wichtig auch theoretische Betrachtungen und Reflexionen sind, so entscheidend sind die vielen kleinen Bausteine, die sich aus den alltäglichen Handlungen und den Konstanten des Alltags ergeben können. Will man verstehen, warum Überwachung funktioniert, wie die Umsetzung von Gesetzen auf Gesellschaft wirkt, wie der Überwachungsstaat

konstituiert ist, dann kommt man an den quantitativen und qualitativen Analysen von Praktiken der Überwachung und Kontrolle nicht vorbei. Will man mit dieser Perspektive Überwachung und Kontrolle untersuchen, bedeutet das, sich in jeweils konkreten Fällen darauf zu konzentrieren wie Überwachung „passiert“ und welche Rolle die Handelnden dabei spielen.

3.2.5 Überwachung als soziale Beziehung / Akteure der Überwachung

Die vorherigen Ausführungen haben deutlich gemacht, dass Überwachung als soziale und kulturelle Praxis die Handelnden und ihre Interpretationen und Deutungen von Technologie und den sie umgebenden Kontext mit einbeziehen muss. Damit ist allerdings noch nichts über das Verhältnis der Akteure untereinander gesagt worden. Die Fortführung einer Betrachtungsweise der kulturellen Praxen im Zusammenhang mit Überwachung bedeutet, sich auf die Formation sozialer Beziehungen zu konzentrieren, die hier entstehen bzw. wie diese generell durch Überwachung konstituiert werden. Jenseits aller Unschärfen des Begriffes der Überwachung (vgl. weiter oben, auch Haggerty 2006; Staples 2014) spricht viel dafür, dass ein Aspekt so gut wie immer zur Qualifikation von Überwachung zutrifft: Überwachung schafft eine Beziehung, die in der Regel ein Subjekt und ein Objekt generiert. Jemand oder eine Technik beobachtet, etwas oder jemand wird beobachtet. Und gehen wir davon aus, dass Überwachung, wie sie hier verstanden wird und Objekt der Betrachtung dieser Expertise ist, sich auf Menschen und ihr Verhalten bezieht, dann wird hier eine soziale Beziehung etabliert (Vande Walle et al. 2012). Diese dichotome Beziehung trifft auf fast alle Formen der Überwachung zu – eine Selbstüberwachung im Sport, beim Training oder an anderer Stelle mag davon ausgenommen sein. Schaut man sich allerdings tiefergehende Diskussionen zur Selbstbeobachtung oder Selbstüberwachung an, dann sind auch diese Formen an die Existenz Dritter gebunden, die diese Selbstbeobachtung initiieren, hervorrufen, abgleichen oder als Referenz nutzen, womit die binäre Opposition von Subjekt und Objekt erhalten bliebe. Dass sich bei einer gegenseitigen Überwachung (vgl. Zurawski 2005; Andrejevic 2005 spricht hier von *lateral surveillance*) die Rollen von Subjekt und Objekt verkehren können, ist selbstverständlich, zeigt aber auch nur die generelle Unbeständigkeit solcher Beziehungen, die eben mit dem Rückgriff auf kulturelles Wissen und soziale Rollen in unterschiedlichen Kontexten neu ausgehandelt werden bzw. sich in und durch diese konstituieren. Die Alltagserfahrungen von Menschen, ihr Handeln und ihre dahinter stehenden Rationalitäten sind deshalb hier von besonderer Bedeutung. Auch wenn eine solche Dichotomie analytisch nützlich ist, so zeigt die empirische Erfahrung, dass die Verhältnisse und Beziehungen doch oft komplizierter sind, zumal wenn es um eine Bestimmung von Objekt und Subjekt geht. Überwachung ist zumindest bi-direktional, wenn nicht vielfältiger. Überwachung als soziale Beziehung ermöglicht eine besondere Form der Kommunikation oder sozialen Interaktion zwischen persönlich an- und abwesenden Personen. Das bedeutet

keinesfalls, dass diese Kommunikation gleichberechtigt ist, aber sie ist vorhanden. Über sie werden die Teilnehmer strukturiert, eingeteilt und erhalten ihre Möglichkeiten zur Partizipation an der Kommunikation. Überwachung beeinflusst Überwacher und Überwachte. Denn in den Alltagserfahrungen, in denen sie handeln wird sowohl Überwachung geprägt, als auch verändert und mit Bedeutungen versehen. Diese Handlungskontexte zu verstehen, bedeutet einen Zugang zu den Interpretations-möglichkeiten von Überwachung und somit auch ein Verständnis zur Bewertung von Überwachungsmaßnahmen und zu deren Wahrnehmung zu gewinnen. Genau deshalb sollte eine Forschung zu Überwachung und auch die Bewertung solcher Maßnahmen oder technischer Innovationen weiter gehen, als nur bis zur Frage, ob etwas effektiv arbeitet oder ob ein Instrument einen panoptischen Effekt hat. Dieser ist so absolut und mit theoretischen als auch populären Annahmen verbunden, dass dahinter die Kommunikationsmöglichkeiten und sozialen Beziehungen zurückstehen müssen, die im einzelnen Fall einem Panopticon geradezu zuwider laufen könnten. Nimmt man diese soziale Beziehung von Überwacher und Überwachten als Ausgangspunkt der Betrachtung, dann muss eine Forschung und Bewertung auf der Kenntnis dieser Beziehung aufbauen. Das bedeutet die Arbeitsabläufe, politischen Wünsche, die Wahrnehmungen und Narrative zu untersuchen, die damit verbunden sind. Nach den Auswirkungen von Überwachungsmaßnahmen zu fragen bedeutet eben nicht über philosophische oder theoretische Konsequenzen zu spekulieren, sondern heißt sich den Erfahrungen von Akteuren zuzuwenden, und wie diese von Politik, den Konsequenzen von Technologien selbst, den Arbeitsabläufen oder rechtlichen Rahmenbedingungen abhängen und beeinflusst werden.

Die konsequente Herleitung einer Betrachtungsweise, die soziale Beziehungen im Zusammenhang mit Überwachung in den Mittelpunkt stellt, könnte folgendermaßen aussehen. Dabei wird auch die Rolle der Technologie selbst berücksichtigt, die (wie oben angesprochen) nicht ursächlich ist, sondern Mittel, Projektionsfläche oder Produkt von Überwachung.

1. **Überwachung ist eine soziale/kulturelle Praktik.** Ob diese durch sich selbst entstanden ist oder (was wahrscheinlicher ist) im Zusammenspiel mit anderen Prozessen muss Kontext-abhängig bestimmt werden.

2. **Überwachung als soziale/kulturelle Praktik konstituiert soziale Beziehungen.**

3. Überwachung ist somit eine eigene soziale Beziehung, die **verschiedene Akteure und Parteien zueinander in Relation** setzt – möglicherweise, aber nicht notwendigerweise hierarchisch.

4. Überwachung als soziale Beziehung kommt in den Praktiken zum Vorschein, **die von Machtverhältnissen innerhalb einer weitergefassten politökonomischen Konstellation geprägt sind.** Das bedeutet, dass Menschen andere Menschen im Auftrag dritter Parteien überwachen.

5. **Technologie in diesen Praktiken wird verwendet, weil:**

   - sie vorhanden ist.
   - sie sich für eine Überwachung nutzen lässt.
   - über sie soziale Beziehungen hergestellt werden, und somit Überwachung entsteht.
   - politische, wirtschaftliche, soziale oder kulturelle Notwendigkeiten bestehen, die eine Verwendung nahelegen.

Technologie kann hier u.U. zu einer Lösung von als Problemen identifizierten Sachlagen dienen. Zu berücksichtigen sind die Wechselwirkungen sowie mögliche Funktionswanderungen von Technologie, d.h. dass eine für ein Problem etablierte technische Lösung auch für andere benutzt wird, bzw. sich eine solche Verwendung in der Praxis herausbildet.

Die Beachtung sozialer Praxen sowie der Zusammenhänge von Überwachung und sozialen Beziehungen (oder als diese selbst) bedeutet eine alternative Perspektive auf das Phänomen, die empirisch neue Möglichkeiten eröffnet und theoretisch an den Alltagserfahrungen im Umgang auch mit Technologie und den daran hängenden Deutungen ansetzt. Diese Perspektive ist auch im Hinblick auf Handlungsempfehlungen von Bedeutung, was an den Beispielen weiter unten noch deutlich gemacht werden soll.

3.2.6 Zusammenfassung: Überwachung als Management gesellschaftlicher Probleme

Der Blick auf die Erscheinungsweisen von Überwachung hat die Vielfältigkeit dieses im Kern als Tätigkeit beschriebenen Phänomens verdeutlicht. Zwischen den theoretischen Modellen, die zur Beschreibung von Gesellschaft auf das Phänomen zurückgreifen bzw. dieses in das Zentrum der Analyse stellen und den Erscheinungsweisen ergibt sich ein sowohl praktischer als auch theoretischer Horizont, der die einzelnen Facetten und Analysemöglichkeiten aufzeigt. Was bisher noch nicht ausreichend thematisiert und klassifiziert wurde sind die Ziele von Überwachung, nämlich die Objekte der Überwachung. Grundsätzlich kann man eine Einteilung in drei Bereiche vornehmen: **Raum**, **Menschen**, **andere** – zu letzterem gehören nicht belebte Objekte wie etwa Gebäude, oder alles was unter die Kategorie „Natur“ fällt (Tiere, Klima, Wasser, Umwelt usw.). Die Kategorien **nicht-belebte Objekte** und **Natur** sind nur dann sozialwissenschaftlich von Interesse, wenn es eine Verbindung zu Menschen

oder Gesellschaften gibt, d.h. diese von einer Überwachung betroffen sind, weil sie sich darin aufhalten oder in irgendeiner Weise nutzen und somit zum Kollateralziel der Überwachung werden. Natur kann auch das mittelbare Ziel der Überwachung sein, um darüber vermittelt Menschen zu kontrollieren, den Zugang zu steuern oder relevante und entsprechend kontextuelle Informationen abzugreifen.

Raum als Bereich der Überwachung ist soziologisch zu verstehen, nämlich als relationale Größe, d.h. als ein belebter und von Menschen definierter Raum (vgl. Löw 2001). Von Menschen definiert heißt in diesem Fall, dass ein physisch erfahrbarer Raum durch Nutzung, Definition (und das bedeutet durch Machtverhältnisse) und Aushandlung bestimmt wird. Ob etwas ein Gefahrengebiet ist oder nicht, ist weder ontologisch feststellbar, noch ist es unveränderlich. Die Überwachung des Raums zielt mittelbar auch auf Personen, aber nur als Nutzer eines Raumes, weniger als näher bestimmte und identifizierte Individuen. Wie in Tabelle 1 bereits gezeigt, sind bestimmte Technologien und Verfahren eher dem einen oder anderen Bereich zuzurechnen. Warum aber nun Überwachung? Wie eingangs bereits geschehen, habe ich Überwachung als Mittel zur Steuerung und Schaffung von Ordnung durch das routinemäßige Sammeln und Verarbeiten von Informationen definiert. Grundsätzlich geht es also darum **Personen zu verwalten**, d.h. **Wissen** anzuhäufen, auf dem Entscheidungen eines Staates, einer Behörde, eines Unternehmens oder einzelner Personen gründen können. Dabei ist Überwachung kein Selbstzweck, sondern im Sinne einer bürokratischen, politischen oder unternehmerischen Rationalität zielgerichtet. Die Aufrechterhaltung von Sicherheit kann so ein Ziel sein. Dazu bedarf es eines **Wissens über die Risiken**, die Sicherheit in einem abgegrenzten Kontext bedrohen könnten. Sofern diese Risiken von Menschen ausgehen oder diese bedrohen, ist ihre Überwachung in der Rationalität gerechtfertigt – im Sinne der binären Qualität von Überwachung, die sich an den Polen Kontrolle und Fürsorge orientiert.

Technologie dient hier als Mittel der Überwachung, die aufgrund der Notwendigkeiten eingesetzt wird, die sich aus den Rationalitäten ergeben. Videokameras zur Kriminalitätsprävention sind kein Machtmittel, eingesetzt um Bürgern auf die Nerven zu fallen oder diese in ihren Bürgerrechten zu verletzen, sondern als Mittel ein soziales Problem (Kriminalität im öffentlichen Raum) zu bekämpfen bzw. zu managen. Überwachung bedeutet nicht die Abschaffung dieser Probleme, sondern zu allererst ist es eine Methode der Wissensgenerierung für Managementprozesse von erkannten Problemen. Erkannte oder mögliche Risiken sollen umgangen werden. Es findet eine Kontrolle von Raum oder Menschen (oder beidem) im Vorwege statt. Im Falle von Überprüfungstechnologien ist der Managementaspekt noch deutlicher, nämlich dann wenn es um Ein- oder Ausschlüsse von Personen oder Personengruppen geht.

Überwachung in diesem Sinne bedeutet die bürokratischen oder unternehmerischen Notwendigkeiten von Sicherheit mittels eines Managements der Risiken zu gewährleisten. In diesem Sinn ist Überwachung ein Mittel der Macht, aber nicht aus sich selbst heraus und nicht als Selbstzweck, sondern in der Anwendung als Mittel eines Managements. Die Form und der Anwendungsbereich der Technologie ergibt sich aus den formulierten Bedürfnissen. Das bedeutet allerdings nicht, dass diese Bedürfnisse ohne Folgen sind und die Konsequenzen immer unabsehbar bleiben. Technologien können anders eingesetzt werden als ursprünglich geplant, Ziele können sich ändern, Rationalitäten politischen Veränderungen unterworfen sein. Deshalb ist Überwachung praktisch angewendet immer nur Mittel zum Ziel, ein **Steuerungsinstrument** von Politik, Unternehmen, Behörden oder in der Umkehrung der Machtverhältnisse auch von Bürgern gegen die Überwachung selbst (vgl. dazu Hempel & Töpfer 2009; Wiedemann 2011; Boghosian 2013; Mackey 2013; Stark & Rosenbach 2014; zur sog. Sousveillance vgl. Mann et al. 2002 und Cardullo 2014; zur Countersurveillance vgl. Monahan 2006 und Wilson & Serisier 2010).

Die Zusammenhänge zwischen den **Zielen**, den politischen/bürokratischen **Rationalitäten**, den **Anwendungsgebieten** und den **Kontrolleuren** der Technologien sind die Eckpunkte für eine Bewertung von Überwachung. Außerdem ermöglichen sie die Beschreibung ihrer Steuerungsmechanismen und ihrer potenziellen Auswirkungen auf Personen, Rechte und Freiheiten.

4. Felder der Überwachung und technische Innovationen – Anwendungsfelder und Intentionen

Um eine Grundlage zur Bewertung technologischer Innovationen im Bereich Sicherheit zu haben, die prinzipiell mit Motiven der Überwachung und Kontrolle verknüpft sind, sollen hier verschiedene Anwendungsfelder beispielhaft beschrieben werden. Die oben genannten Zusammenhänge zwischen den **Zielen**, den politischen/bürokratischen **Rationalitäten**, den **Anwendungsgebieten** und den **Kontrolleuren** der Technologien sind die Eckpunkte, um Überwachung exemplarisch deutlich zu machen. Da es in der Expertise hauptsächlich um eine zivile Sicherheit geht, eignen sich als Felder der Flughafen einerseits und die Stadt andererseits. Beides sind vielfältige und komplexe Infrastrukturen, die sich in der Nutzung, Wahrnehmung und den Formen der Überwachung deutlich unterscheiden. Bei der Stadt geht es vor allem um eine Überwachung von Infrastrukturen und von öffentlichen (und privaten) Räumen. Da im Zuge der Digitalisierung der Lebenswelten, unserer Umwelt und letztlich auch durch die Digitalisierung der Gesellschaften selbst, diese Technologien und Anwendungen eine zentrale Rolle spielen, wird in diesem Zusammenhang als weiteres Anwendungsfeld auch das so genannte Internet der Dinge thematisiert und vorgestellt. Nicht zuletzt, weil dieses in der Betrachtung des Konzeptes so genannter *smart cities* und damit im Hinblick auf eine Überwachung von Infrastrukturen eine wichtige Rolle spielt. Beim Flughafen handelt es sich um eine relativ abgeschlossene Umgebung, die von ihrer Bedeutung her jedoch weit über den eigentlichen Raum hinauswirkt, insbesondere wenn es um Formen und Technologien der Überwachung geht. Auch Flughäfen sind urbane Infrastrukturen, die im Sicherheitsdiskurs auch als so genannte kritische Infrastrukturen bezeichnet werden. Sie sind Teil von Städten und *smart cities*, dann allerdings als Ganzes, während hier der Unterschied anhand der internen räumlichen Strukturen gemacht werden soll – System Flughafen vs. System (smarte) Stadt.

Gemeinsam ist beiden Anwendungsfeldern – Flughafen und (smarte) Stadt –, dass es sich um Räume handelt, in denen der Aspekt von Menschenströmen grundlegend ist. Damit ist aber noch nicht gesagt, wie sich diese Räume konstituieren, welche Handlungsmöglichkeiten sich den Menschen bieten, welche materiellen Grundlagen eine Rolle spielen und was diese für eine Überwachung ganz praktisch bedeuten. Bevor die Räume selbst beschrieben werden, wird deshalb zunächst als Grundlage für die weiteren Ausführungen die Bedeutung des Raumbegriffes für eine Analyse von Überwachung geklärt.

4.1 Raum und Überwachung

Einen umfassenden Raumbegriff an dieser Stelle vorzustellen würde den Rahmen der Expertise sprengen. Noch fast jede Disziplin hat ihren eigenen Raumbegriff geprägt, die mal anschlussfähig aneinander sind, mal sich gegenseitig ausschließen. Gemeinsam ist ihnen, dass sie versuchen eine materielle Größe zu fassen (manchmal auch eine immaterielle mit materiellem Bezugspunkt (vgl. zu dieser Verbindung auch Miller 2005 Materiality) zu erklären und für eine wissenschaftliche Analyse brauchbar zu machen. So gibt es Raumdefinitionen dort, wo sie selbstverständlich erscheinen, in der Geographie, Architektur, Kartographie, Soziologie, Ethnologie, Physik oder Mathematik, aber auch dort, wo sie eher nicht sofort angenommen werden, z.B. in der Psychologie und Theologie (für eine Übersicht vgl. Günzel 2006; auch Dünne & Günzel 2006). Zumeist geht es in den Definitionen darum zu verstehen und zu beschreiben, wie die Dimension Raum begriffen werden kann, sei es als soziales Konstrukt oder als eine von verschiedenen Dimensionen der physischen Umwelt, wie es die Geographie auch noch, aber nicht ausschließlich macht (vgl. Hubbard et al. 2002). Die in den Definitionen festgehaltene Beschaffenheit von Raum entscheidet mit über die Verwendung von Raum, den Umgang mit ihm und den sich im Raum befindenden Menschen und Gütern. Begreift man beispielsweise einen Flughafen als eine Art Theaterbühne, auf der die einzelnen Personen in den ihnen zugewiesenen Rollen agieren, dann haben die Handlungen selbst nichts mit der Beschaffenheit des Raumes zu tun. Bestenfalls ist der Raum so gestaltet, dass er bestimmte Handlungen erzwingt, z.B. über Absperrungen, Einbahnwege, Verkehrsführung. Die Annahme, dass der Raum durch die sozialen Handlungen selbst erst von den in ihm handelnden Personen geschaffen wird, hat in einer fixierten (auch als absolut bezeichneten) Raumvorstellung keinen Platz. Aber gerade die Vorstellungen, dass ein Raum nicht nur das ist, was seine vermeintlich neutrale geometrische und physische Beschaffenheit ausmacht, sondern, dass er auch durch die Handlungen der darin an- und abwesenden Personen gemacht und definiert wird, neu angeeignet und möglicherweise in den sich ergebenden Praktiken neu gedeutet wird, ist in der Folge zentral. Das gilt insbesondere für im Raum stattfindende Praktiken der Überwachung, die mit den Vorstellungen über Raum eng verbunden sind. An den Beispielen Flughafen und Stadt wird das in den folgenden Abschnitten noch deutlicher werden. Hier soll zunächst erst einmal eine Definition von Raum vorgestellt werden, die als Arbeitsgrundlage dienen soll.

Löw (2001) hat Raum als soziale Größe umschrieben, die durch die Beziehung von Handlungen und Anordnungen gleichermaßen bestimmt wird. Als soziologischer Begriff ist Raum keine feste physische Größe, in der Menschen unabhängig von ihm handeln, sondern Raum ist selbst Teil der Handlungen und wird durch diese erst konstruiert. Ein solcher relationaler Raumansatz hat sich in den letzten Jahren in vielen Disziplinen durchgesetzt (vgl. auch Glasze, Pütz & Rolfes 2005; Schroer 2006; Klauser

2006; Belina 2007). Dabei wird an vorherige Konzeptionen von Lefèbvré (1968), Raffestin (1980 zitiert in Klauser 2006: 100ff) und Soja (1989, 1996) angeschlossen (vgl. auch Werlen 2009). Raum ist insoweit eine soziale Größe, als er einerseits einen Bezugsrahmen für menschliches Handeln bereitstellt und andererseits durch soziales Handeln erzeugt und gestaltet werden kann. Damit ergibt sich ein Problem. Nämlich die Frage, ob Raum gänzlich aus der Anordnung sozialer Beziehungen heraus entsteht, oder ob zu diesen Anordnungen auch die physische Umwelt und die kognitiven Vorstellungen gehören, die einen Raum auch ohne die sozialen Handlungen konstituieren und welche Wechselwirkungen es zwischen diesen Formen der Räumlichkeit gibt. Eine Antwort darauf ist für die Untersuchung von Raumvorstellungen und ihren Repräsentationen wichtig, da Vorstellungen auch von den Bedingungen physischer Erscheinungen und ihrem symbolischen Gehalt abhängen. Insbesondere letztere werden erst unter bestimmten sozialen Bedingungen in der einen oder anderen Art wahrgenommen und einer qualitativen Wertung unterzogen (vgl. u.a. Wassman 1993; Wassmann & Dasen 1998). Materielle Bedingungen eines Raumverständnisses können auch dazu dienen, ein Modell für die Orientierung im Raum und somit gleichsam eine Blaupause für mögliche Handlungsoptionen zu liefern, die dann wiederum auf den Raum einwirkt. Räumliche Anordnungen werden darum ebenso von den gesellschaftlichen Strukturen vorgegeben wie sie diese mit prägen. Naturräumliche und künstlich hergestellte physische Tatsachen von Räumen sind insofern von Bedeutung als sie soziale Handlungen beeinflussen können. So können Räume oder räumliche Elemente Grenzen setzen, um damit ein Innen und ein Außen herzustellen. Diese Grenzen bestimmen nicht in deterministischer Weise das jeweilige soziale Handeln. Aber sie sind ein Teil der räumlichen Anordnung, mit denen soziales Handeln zurechtkommen muss, durch den es sich verändert oder den Raum selbst neu interpretiert oder neu ordnet. Physische, durch den Raum gegebene, Grenzen oder auch in den Raum hineingesetzte Grenzen sind häufig Mittel von Macht und Herrschaftskontrolle, wie zum Beispiel die Grenzen rund um die palästinensischen Gebiete, über die Israel die eingeschlossenen Gebiete und die darin lebenden Menschen kontrolliert (vgl. Algazi 2008: 311ff; vgl. auch Zureik 2010). Die grundsätzliche Unterscheidung von Form und Funktion, von Beschaffenheit und Bedeutung, und deren Beziehung darf nicht der grundsätzlichen Annahme von räumlichen Konstruktionen hinterherhinken. Dennoch, so gibt Werlen zu bedenken, sollte bei der Begriffsbestimmung darauf geachtet werden, dass die Konzepte nicht vermischt werden – also physisch-geographische Wirklichkeiten nicht durch soziale Raumkonzepte erklärt werden und umgekehrt. Es sei daher nicht möglich, vom physisch-materiellen Raum im Sinne einer materiellen Entität zu sprechen (Werlen 2009: 152). Dennoch sei *„von einem handlungszentrierten Standpunkt aus Raum als eine begriffliche Konzeptualisierung der physisch-materiellen Wirklichkeiten zu verstehen“*, die wegen der Körperlichkeit der Subjekte von Bedeutung ist. Deutlich wird in diesen Ausführungen, dass Raum nicht nur durch Handlungen erklärt werden kann, eine alleinige soziologische Konzeption

nicht reichen würde. Der physische Raum, gerade wenn es um seine Interpretation durch Menschen geht, und daran anschließende Veränderungen im Hinblick auf Kontrolle, Einschließungen oder Ausgrenzungen, ist ebenfalls enorm wichtig. Die Materialität der physischen Umwelt muss auch für einen soziologischen und andere darauf aufbauende Raumbegriffe von Bedeutung sein. Denn nur dann können die Beziehungen zwischen dem physischen Raum und den ihm gegebenen Bedeutungen adäquat analysiert und beschrieben werden. Die Materialität eines Raumes ist dabei nicht als Staffage zu verstehen, als Hintergrund auf und vor dem gehandelt wird, sondern sie ist Teil der Handlung, wenn nicht sogar die Handlung selbst.

Auch Überwachungs- und Kontrollmaßnahmen können einerseits mit vielfältigen Eingriffen in den Raum einhergehen, andererseits können räumliche Bedingungen zur Kontrolle und Überwachung genutzt werden. Letzteres würde bedeuten, dass räumlichen Elementen neue Bedeutungen gegeben werden, die wiederum soziales Handeln beeinflussen. Blickt man aus der Perspektive der Überwachung auf den Raum, dann handelt es sich häufig auch um Territorien, einen konkreten Ort oder einen nicht näher definierten Raum im nicht-territorial verankerten Sinn. Im Fall von Überwachung geht es um seine narrativ-diskursive Bedeutung und die – durch die Wahrnehmungen gesteuerte – Ausgestaltung und ihre (räumlichen) Konsequenzen (z.B. im Falle von Überwachungsmaßnahmen oder der Stigmatisierung als so genannte Kriminalitäts-brennpunkte). Es muss also möglich sein, einen Raum in seiner Materialität zu beschreiben, um darauf aufbauend die ihn umgebenden Konzepte, Interpretationen und Funktionen zu analysieren. Materialität und Interpretation, also die sozial gefilterten Wahrnehmungen der physisch-materiellen Wirklichkeiten, bedingen sich dabei gegenseitig und führen erst zu dem, was wissenschaftlich mit unterschiedlichen Raumbegriffen erklärt wird und alltagspraktisch in verschiedenen Wahrnehmungen und Diskursen von Räumlichkeit zum Ausdruck kommt.

Raum wird nach Marx (2005) im Zuge der neuen Formen der Überwachung zu einer Kategorie von Kontrolle und Überprüfung (vgl. auch Haggerty & Ericson 2006, Lyon 2007). Der Unterschied von neuen und alten Formen der Überwachung besteht hauptsächlich im Verhältnis zu Objekten der Überwachung sowie ihren Strukturen. Vom reinen Kontrollaspekt haben sich technologische Überwachungspraktiken und ihre gesellschaftlichen Pendants immer mehr zu Überprüfungs- und Steuerungsinstrumenten entwickelt, die an Kategorien, Mustern und Gruppen interessiert sind (vgl. Marx 2004, Samatas 2004, Zurawski 2014). Damit ändert sich auch der Fokus, der nun vorrangig kontextbezogen ist und sich auf Räume, Orte, Zeitabschnitte und Kategorien von Personen konzentriert (vgl. auch Graham & Wood 2003). Es werden Kategorien überwacht bzw. deren Auftreten und Verhalten überprüft. Angesichts riesiger Daten-sammlungen und den Auswertungsalgorithmen innerhalb von Überprüfungsregimen scheint Raum seine konkrete Bedeutung und materielle Qualität zu verlieren und zum

Raum der Wahrscheinlichkeiten zu mutieren (vgl. Bogard 2006, 59). Während es bei Foucault noch konkrete Räume waren, innerhalb derer fest umrissenen Grenzen diszipliniert wurde, und in denen die Überwachung quasi in den räumlichen Anordnungen eingeschrieben war, sind es nun die Beziehungen und definitorischen Konstruktionen von Räumen, die einer Überwachung unterliegen. Ein physischer Raum, kann nach der Logik neuer Überwachungsformen verschiedene Kategorien bilden, je nachdem mit welchen Daten er kombiniert wurde. Es geht nicht mehr um die bloße Disziplinierung von Menschen und Gesellschaften, sondern um die Kontrolle einer nur angenommenen Konformität, eines Idealbildes, welches tatsächlich nur in der Phantasie oder einer Simulation existiert (vgl. Zurawski 2007b).

Die konkreten Praktiken der Überwachung und Kontrolle sind räumlich und sozial begründet, sie konstruieren und formen gleichermaßen Räume und räumliche Vorstellungen. Solche Rückkoppelungen können in selbstreferentieller Weise die Begründung einer Kontrolle gleich mitliefern (*„an kriminellen Orten sind Kameras, die darauf hinweisen, dass dort ein krimineller Raum sein muss, weshalb er überwacht werden darf*“, siehe Kapitel 3). Es entstehen eventuell neue räumliche Interpretationen, die wiederum Grundlage für neue Elemente sozialen Handelns und sozialer Beziehungen sein können. Raum ist jedoch nicht allein sozial konstruiert und von sozialen Handlungen abhängig, sondern als physisch-kognitiver Bezugsrahmen auch für die Ausgestaltung sozialer Wirklichkeiten wichtig. Um die Beziehungen von Weltbildern und Überwachung zu untersuchen, sind soziales Handeln und physisch-räumliche Bedingungen als eine Einheit zu sehen. Denn die Überwindung von Grenzen – sozialen und physischen – ist geradezu ein Grundmerkmal von Überwachungspraxen. Am Beispiel öffentlicher Videoüberwachung will ich das kurz illustrieren.

Videoüberwachung und Raum – verstanden als territoriale Vorstellungen eines konkret verortbaren Raums – hängen eng miteinander zusammen. Die Kameras überwachen Orte (öffentliche Plätze und Straßen) – fest umrissene physische Räume, in denen Menschen sich bewegen, aufhalten oder leben. Der überwachte Raum wird so als feste, messbare Größe angenommen, in etwa wie ein Container, in dem soziale Handlungen ablaufen, die dann beobachtet werden und entsprechend festgelegter Normen bewertet werden. Dass es sich hierbei um eine an der Wirklichkeit gesellschaftlichen Lebens vorbeigehende Sichtweise handelt, ist offensichtlich. Denn Orte sind abhängig von den Handlungen der Menschen, die eine soziale oder persönliche Beziehung zu dem Raum aufbauen. Ihr Verhalten richtet sich nach den Normen und Erwartungen, die an öffentliche Orte geknüpft sind und daran welche Bedeutung dieser Raum zum Zeitpunkt des Handelns für sie hat. Die essentielle Annahme von (fixen) Räumen, die in ihrer physischen Beschaffenheit beschrieben werden können, erscheint so gesehen konsequent. Im Kern einer solchen Auseinandersetzung geht es aber eigentlich um die Frage, wer die Hoheit über die Definition besitzt, was einen Raum ausmacht und wer

ihn wie bestimmen und letztlich auch benutzen darf. Erwartungen und Bedeutungen jedoch sind eher weiter als enger gefasst. Eine Überwachung, die nur festhält, was an dem als „Kriminalitätsschwerpunkt“ definierten Ort passiert, nicht aber evaluiert, ob diese Annahme überhaupt gerechtfertigt ist, legt den so bestimmten Ort auf diese Funktion fest und verengt die Normen, ohne dass sich die dort aufhaltenden Menschen dieser Normeneinschränkung bewusst sind. In den meisten Fällen von Videoüberwachung ist ein solcher Raum territorial gebunden. Der Raum oder spezifische Ort wird als „Kriminalitätsschwerpunkt“ per Definition geschaffen und gleichermaßen kriminalisiert (Czerwinski 2007; Czerwinski & Zurawski 2008). In einem solchen „Kriminalitätsraum“ handeln Menschen – so die Annahme der Überwacher – nach dem Entweder-oder-Prinzip, etwas anderes ist nicht vorgesehen. Nun ist öffentliche Videoüberwachung keine geheime Veranstaltung, sondern den Menschen bekannt, nicht jedoch die Parameter und Normen der Abweichung und Kategorien der Aufmerksamkeit, nach denen überwacht wird. Die Kamera ist ein materielles Gut und ihre Existenz in gewisser Hinsicht auch eine soziale Handlung, welche auf das Handeln von Menschen einen Einfluss hat und zu neuen Interpretationen, Handlungen und Wahrnehmungen führen kann. Darüber hinaus setzen Kameras Grenzen (Klauser 2006). Sie teilen Orte in solche mit und solche ohne Kameras ein, was in der Konsequenz zu neuen Räumen und Raumbildern führen kann. Ein „Kriminalitätsschwerpunkt“ wird durch die Definition erst dazu gemacht, ungeachtet der Bedeutungen und Vorstellungen, die sonst noch von diesem spezifischen Ort existieren können. Die Kennzeichnung als „gefährlich“ aber bringt wieder neue Vorstellungen hervor, beeinflusst möglicherweise die Wahrnehmung und damit das soziale Handeln von Menschen an dem Ort, vielleicht sogar die physische Umgestaltung des Ortes selbst. Die Begründung für die Kameras wird mit ihrer Installation gleichermaßen gegeben, denn nur dort, wo Kameras sind, seien sie demnach auch nötig.

Anhand der Räume Flughafen und Stadt wird deutlich, dass es eine Vielzahl an Wechselwirkungen geben kann, die mit den jeweiligen Besonderheiten der Räume selbst, ihrer Bedeutung für die Menschen, den sie umgebenden Diskursen sowie den Handlungsmöglichkeiten zu tun haben. An Flughäfen wird die Nutzung des Raumes von der Spannung zwischen den Anforderungen der kommerziellen Aspekte des Flugverkehrs und der Rhetorik der Sicherheit bestimmt. Die kommerziellen Anforderungen umfassen u.a. die Passagiere problemlos und schnell zu den Fliegern zu bringen, sie dabei so intensiv wie möglich an den vorhandenen Geschäften vorbeizuführen und entsprechend ein Populationsmanagement entsprechend effizient zu organisieren. Die Rhetorik der Sicherheit steht in einem Spannungsverhältnis dazu, da alle Handlungen, die Architektur, Arbeitsabläufe und das Management der Passagiere und Beschäftigten auch danach ausgerichtet sein müssen, Sicherheit und kommerzielle Interessen zusammenzubringen. Die Nutzung des Raumes wird davon grundlegend bestimmt – und darüber auch die Normen, mögliches abweichendes Verhalten, die

Formen der Überwachung sowie letztlich auch die Wahrnehmung von Sicherheit an diesem Ort.

4.2 Flughafen

Will man Sicherheit an Flughäfen beschreiben, dann ist das für den Passagier auffälligste die Sicherheitskontrollen, die mehr oder weniger ähnlich rund um die Welt stattfinden: Menschen werden in Schlangenlinien sortiert und aufgereiht zu den Röntgengeräten, den Scannern, den Kontrolleuren geleitet. Standardisierte Fragen nach Flüssigkeiten oder Anweisungen zum Durchschreiten der Torbogensonden (Abnehmen des Gürtels, Ablegen von Mobiltelefonen u.a.) helfen den Passagieren und Kontrolleuren gleichermaßen. Es sind Praktiken der Sicherheit bzw. der Sicherheitskontrollen, die hier vollzogen werden, die sich an diesen Orten im Zusammenspiel mit Technologien herausgebildet haben und zum Repertoire von Reisehandlungen gehören. An allen Flughäfen der Welt wird eine ähnliche Prozedur erwartet, was dabei insbesondere dem effizienten Management der Passagiere hilft. Und auch die Technik ist im Wesentlichen die gleiche: Torbogensonden, Gepäckscanner, manchmal Körperscanner und Irisscanner, dazu das Personal, welches die Abfertigung managt. Sicherheit spielt am Flughafen in jedem Fall eine zentrale Rolle, nicht nur in der Luft, sondern lange vor dem eigentlichen Flug. Dass es um Sicherheit geht, ist jedem Fluggast. Dabei geht es an diesen Passagierschnittstellen vor allem um die Abwehr von Gefahren, die mittlerweile zu einem elementaren Teil des Fliegens geworden sind. Die Beherrschung damit verbundener Risiken gehört dazu und bestimmt in unterschiedlichen Aspekten das Phänomen des Fliegens zentral mit.

Nicht erst seit dem 11. September 2001 ist der Flughafen so zu einem Synonym für den Umgang mit Sicherheit geworden, auch weil Flughäfen Orte sind, an denen globale Mobilität und Grenzübertritte organisiert und gemanagt werden müssen. Flughäfen sind *„the most stringently surveilled sites in terms of the means of movement and identification“* (Lyon 2008, 34). In diesem Sinne sind sie Räume der Überwachung und Kontrolle par excellence. Bereits vorher gab es Anschläge auf Flugzeuge, die durch die Umgehung von Sicherheitsmaßnahmen an Flughäfen ermöglicht wurden. Budd et al. (2015, auch 2009, Warren 2010) liefern eine historische Aufarbeitung von Flugsicherheit im weitesten Sinne, die allerdings eng an eine geografische Sichtweise gekoppelt ist. Anhand der Maßnahmen zur Seuchenvermeidung, einer der wohl ältesten Sicherheitsmaßnahmen im Zusammenhang mit Fliegen, zeigen die Autoren wie sich auf diesem Feld Sicherheitsdiskurse entwickelt haben, die nur sehr spärlich ins Bewusstsein der Passagiere dringen, meistens dann, wenn es vermeintlich globale Epidemien gibt, die erst durch den Flugverkehr überhaupt zu solchen wurden oder werden. Jüngste Beispiel dafür sind SARS oder der Ebola-Virus in Westafrika. Weder die Felder, noch die Subjekte von Sicherheit sind festgelegt und unveränderlich. Das zeigen sowohl die

historische Entwicklung, als auch das Thema der Epidemien und ihrer Überwachung selbst, welches sich mit Blick auf Viren und Hygiene von den Gefahren durch Terror und Gewalt unterscheidet (vgl. Budd et al. 2009).

Aber die Anschläge auf das World Trade Center haben dazu beigetragen Sicherheit, insbesondere vor Terror, zu einem der zentralen Aspekte des Fliegens zu machen (vgl. u.a. de Lint 2008; Maguire 2014). Ein weiterer Aspekt, der in dieser Expertise nur von untergeordneter Bedeutung sein soll, ist der Konsum, d.h. der Flughafen als Erlebnisort, über den Distinktion, Lebensstil, Konsum und soziale Ordnung verhandelt und dargestellt werden (vgl. z.B. Adamowsky 2010). Sicherheit als Diskurs ist nicht zuletzt durch die implementierten Technologien der Überwachung, des Flughafen-Managements und der verschiedenen Kontrollen dem Fluggast jederzeit präsent. Auch jenseits der Räume, die ein Fluggast betreten kann, finden sich jede Menge Technologien, die hier allerdings weniger von Bedeutung sein sollen. Zumeist handelt es sich hierbei um das, was anfangs als *safety* bezeichnet wurde, d.h. es geht um die technische Sicherheit des Flugzeuges und des Luftraumes und nur zu einem kleineren Teil um eine Überprüfung von Personen und Gepäck. Der Teil eines Flughafens allerdings, der dem Fluggast zugänglich ist, bzw. in den er nach vielfältigen Überprüfungen gelangen kann, ist gesättigt mit Sicherheitsmaßnahmen und entsprechenden Technologien. Welcher Raum hierdurch erzeugt wird, inwiefern Sicherheit dabei eine Rolle spielt und welche Bedeutung dabei den handelnden Personen zukommt, möchte ich hier skizzieren. Dabei liegt der Fokus auf den Zusammenhängen von Sicherheit, Raum und den Kontrollen auf der einen und den Passagieren und Beschäftigen auf der anderen Seite. Anders als in den ersten Jahrzehnten des motorisierten Flugverkehrs bedeutet Fliegen heute – in aller Regel – kein Abenteuer mehr; dafür jede Mengen Routinen und erlernte Vorgänge, die von einem komplexen System aus Arbeitsabläufen und Techniken verursacht, gesteuert oder möglich gemacht werden. Vom Kauf des Flugtickets, über das Einchecken, dem Passieren der Sicherheitsmaßnahmen und den Gepäckkontrollen bis hin zum Drink an Bord, hat sich das Fliegen zu einer kulturellen und sozialen Praxis entwickelt, die bestimmte Lebensstile und biographische Entwürfe bedingt bzw. erst ermöglicht, und den Takt des Lebens mitbestimmen kann, auch wenn das Fliegen zumeist noch nicht so selbstverständlich ist wie die Mobilität mit Bahn oder Auto. Erfahrungen rund um das Fliegen spiegeln sich in unterschiedlichen alltagskulturellen und populären Quellen, sei es in Spielfilmen, Romanen oder anderen Medien (beispielhaft hier die beiden Kino-Erfolge der letzten Jahre „Terminal“ von Steven Spielberg und „Up in the Air“ von Jason Reitman). Eine Rubrik bei Spiegel-online „Flugzeug-Anekdoten“ oder Sachbücher von Menschen, die über ihre Erfahrungen am Arbeitsplatz Flugzeug schreiben, verweisen auf Reflexionen und Reflexionsbedarf. So hat sich unter dem Label des *mobility turn* vor allem in den Kulturwissenschaften ein Mobilitätsverständnis entwickelt, das *„Kultur aus der Perspektive der Bewegung unter der Bedingung vermehrter Beweglichkeit “ (Rolshoven 2011, 54)* deutet. Dazu gehört

auch die Berücksichtigung des Aspektes der Sicherheit, ein Bereich der in den Kulturwissenschaften hierzulande noch wenig Beachtung gefunden hat, anders als in anderen anthropologischen Traditionen (vgl. dazu u.a. Maguire et al. 2014). Was den Bereich des Fliegens selbst angeht, so ist er ganz selbstverständlich Gegenstand wissenschaftlicher Betrachtungen. Neben den Sicherheitsmaßnahmen an Flughäfen, findet dabei die Architektur von Flughäfen mit ihrer vermeintlich einheitlichen globalen Konsumkultur eine besondere Berücksichtigung, und auch das Design von Flugzeugen ist durchaus Thema. Und doch steht die kulturwissenschaftliche Auseinandersetzung auch hier noch am Anfang. Dieser Band ist auch als Anstoß gedacht, um diesen Mangel zu beheben. Das Beispiel Flughafen und speziell die Sicherheitskontrollen boten sich dabei im Besonderen als Chiffre an, um anhand der Deutungen, Konstruktionen und verschiedenen Dimensionen von Sicherheit deren Spannbreite zu verdeutlichen und zu zeigen, wie sie sich an einem ganz speziellen Ort manifestiert. Je nach Land und Flughafen beginnen die Kontrollen der Passagiere bereits bei der Anfahrt (wie z.B. in Israel), beim Eintritt in das Flughafengebäude, spätestens aber beim Check-In selbst. Die Architektur, insbesondere die „Innenausstattung“ eines Flughafens sind, bei allem Design und Zeitgeist, vor allem auf ein Management von Menschenströmen ausgerichtet. Warteschlangen, Check-Ins, die Sicherheitsschleuse, Passkontrollen, Wege zu und von den Terminals, Abflug und Ankunft. Jeder dieser Bereiche ist für den Passagier eine Sicherheitserfahrung (neben einer ebenfalls vermittelten Konsumerfahrung, deren Implikationen hier den Rahmen sprengen würden), deren Sinn nicht immer voll und ganz nachvollzogen werden kann. Da aber nur eine Wahl zwischen Fliegen oder Nicht-Fliegen besteht, müssen diese Kontrollen akzeptiert werden (vgl. dazu u.a. Herlyn 2015; Vukelic 2015).

Die Sicherheitskontrolle, der Sicherheitsbereich und ganz allgemein die Sicherheit an Flughäfen haben dabei eine zentrale Bedeutung, sowohl in der Praxis als auch in den herrschenden Diskursen. Kaum ein Bereich alltäglichen Lebens ist dermaßen mit dem Attribut Sicherheit versehen wie ein Flughafen. Das liegt zum einen daran, dass Flugzeugunfälle (*safety*) immer spektakulär sind, Flugzeugentführungen (*security*) seit den 1970er Jahren eng mit einem Terrorismus verbunden sind, der sich gegen den Westen richtet, aber auch, weil es sich hierbei um eine Technik handelt, die auf den ersten Blick die Kräfte der Natur überwindet und als ein Wunder der Moderne (Adamowsky 2010) gilt, das Natur und Mensch gleichermaßen herausfordert. Als Technik ist Fliegen ein Modernisierungsrisiko, hat das Potenzial zum Unfall und muss gerade deswegen beherrschbar gemacht werden (wobei ein Kostendruck seitens der Airlines auch hier negative Effekte haben könnte) – vor allem technisch, aber auch diskursiv. Auch wenn dieses Gefühl der Herausforderung weitgehend aus den Diskursen verschwunden ist, so bleibt ein Rest dennoch vorhanden, ein Rest, der ausreicht, um das Thema Sicherheit zu einem elementaren Aspekt des Fliegens und seiner transglobalen Verbindungsorte, den Flughäfen, zu machen.

Die direkte Konfrontation mit Technologien, die als Technologien der Sicherheit beschrieben werden können, ist an Flughäfen sehr direkt und Teil des Fliegens selbst. Die auch anderswo omnipräsenten Videokameras (vgl. z.B. Wagenaar & Boersma 2012) sind dabei nur ein Teil der verwendeten Sicherheits-Technologien. Unzählige Arten von Scannern erfassen das Gepäck und an verschiedenen Stellen das Ticket, welches als Eintrittskarte sowohl in die Warteschlange vor der Sicherheitsschleuse, als auch später in das Flugzeug selbst gilt. Die Sicherheitsschleuse ist der zentrale Punkt einer Sicherheitserfahrung für den Fluggast: Das Handgepäck wird durchleuchtet, die Passagiere im Torbogen auf verdeckte Metallgegenstände hin überprüft. Mittlerweile haben Körperscanner (vgl. u.a. Ammicht Quinn & Rampp 2009; Ammicht-Quinn et al. 2010; Bellanova & Fuster 2013; Nagenborg 2014; Hirschberger 2015) diese Aufgabe an vielen Flughäfen übernommen. Passagiere werden zusätzlich abgetastet, einzelnes Gepäck wird u.U. auf Sprengstoffreste hin untersucht, Polizei und Sicherheitspersonal interviewen einzelne Fluggäste, es wird (wie z.B. in Israel) eine Passagierdifferenzierung durchgeführt, die auf menschlicher Bewertung beruht, anstatt ausschließlich auf der Kontrolle durch Technologien (vgl. Wagner & Bonß 2014). Die Praktiken sind geprägt von Kontrolle der Bewegungen, von der Zurichtung der Passagiere entsprechend der Erfordernisse der Technologien (eingeschlossen sind dabei auch die Arbeitspraktiken des Personals), von einem Management des Passagiers, seinen Bewegungen, Aktivitäten und der Mobilität im Raum selbst (vgl. u.a. Adey 2004, 2010). Durch mögliche Anpassungen des Raumes an die Bedürfnisse der Sicherheitskonzepte, wie möglicherweise eine frühzeitige Trennung der Passagiere durch Klassifikationen wie „vertrauenswürdig“ oder „bedenklich“), verändert sich auch der Raum und mit ihm die Benutzung durch die Passagiere. Der Checkpoint of the Future der IATA könnte unter diesen Aspekten als eine Idee der Umsetzung hier auch Erwähnung finden (vgl. Herlyn & Zurawski 2015a).

Vergleicht man einen x-beliebigen Flughafen mit einem Bahnhof, dann werden diese Erfordernisse sehr augenscheinlich. Bahnhöfe, Orte des Transits, der Begegnung, Thema literarischer Abhandlungen über die mobile Gesellschaft und die Räume der öffentlichen Mobilität (vgl. Künzli 2007), wären nicht praktikabel denkbar unter den gleichen Bedingungen, wie sie an Flughäfen vorzufinden sind, – nicht in Deutschland, an anderen Orten und Verbindungen kann es da durchaus Ausnahmen geben. St. Pancras in London, das Terminal, an dem der Eurostar seine Reise durch den Eurotunnel nach Frankreich beginnt, ist aus Sicherheitsgründen einem Flughafen-Terminal nachempfunden und ähnelt damit keinem gewöhnlichen Bahnhof. Insgesamt verändert sich dort die gesamte Atmosphäre, da alle Handlungsmöglichkeiten eingeschränkt werden, die Technologien entsprechende Anpassungen von den Reisenden verlangen und somit ein anderer Raum entsteht, der letztlich aber als abgetrennter Teil eines klassischen Bahnhofs mitten in London existiert. Sicherheit und der Raum Flughafen sind untrennbar miteinander verbunden. Der Flughafen kann allerdings auch als Vorbild für

Sicherheitskonzepte dienen, die an anderen konkreten Orten und Räumen so gar nicht umgesetzt werden können, da die Möglichkeiten der Kontrolle, Steuerung und des Managements von Personen und Gütern so nicht bestehen, der Wunsch nach Sicherheit und Kontrolle allerdings vorhanden ist. Schlepper et al. (2015) haben für den Fährverkehr gezeigt wie die Konzepte der Mobilitätssicherheit am Flughafen eine Blaupause für andere Bereiche bereitstellen. Diese Analyse macht über den eigentlichen Forschungsgegenstand des Hafens insbesondere deutlich, welche diskursive Wirkung eine Versicherheitlichung von Flughäfen und des Fliegens im Allgemeinen haben kann, wenn die Maßnahmen als Modell für ganz andere Bereiche herhalten müssen, ihrer Umsetzung aber wirtschaftliche und logistische Akzeptanzgrenzen gesetzt sind.

Mit einigem Abstand betrachtet, folgen Sicherheitskontrollen an den Flughäfen rund um die Welt den Standards der IATA und doch gibt es lokale, nationale oder supra-nationale Vorschriften, die davon abweichen können, wie z.B. die europäische Verordnung zur Mitnahme von Flüssigkeiten. In Israel gilt diese Regel zum Beispiel nicht. Am Flughafen Ben Gurion in Tel Aviv, der ansonsten der Inbegriff für Sicherheit, Kontrolle und Überwachung ist, dürfen Flüssigkeiten mitgeführt werden. Dafür stößt das dort durchgeführte Profiling – also die aktive, positive oder auch negative Diskriminierung von Fluggästen – nach einem dem Gast nicht ersichtlich werdendem Muster auch vor Ort selbst auf nur minimale Gegenwehr. Dass eine solche aktive Passagier-differenzierung durchaus als *social sorting*-Praxis gesehen und analysiert werden kann, haben u.a. Herlyn (2014, 2015) und Adey (2004, 2010) ausgeführt. Generell kann aber gefolgert werden, dass auch der geopolitische Kontext und die lokale bzw. nationale Sicherheitskultur Einfluss auf das wie und warum der Kontrollen selbst haben. Auch von Interesse in diesem Zusammenhang ist die Studie von Schaefer (2015) zur Bedeutung von Sicherheitsmaßnahmen angesichts von Behinderung, z.B. bei Roll-stuhlfahrern. Anhand einer ethnographischen Fallstudie zeigt sie anschaulich die Möglichkeiten, Grenzen und Widersprüche von Sicherheitskonstruktionen, die hier gerade durch die Störung des Systems so offen zu Tage treten. Es folgt ein kurzer Exkurs, der die Bedeutung von Kultur für die Wahrnehmung und die Praktiken der Sicherheit aufzeigt (für eine ausführliche Analyse vgl. Herlyn & Zurawski 2015a), insbesondere, was das *social sorting* im Raum Flughafen betrifft.

Die Grundidee der Passagierdifferenzierung wie sie die IATA in ihrem Konzept des *Checkpoint of the Future* vorsieht bleibt im derzeit aktuellen Entwurf, der so genannten *Smart Security* (SmartS) bestehen (Stand Ende 2013)[6]. Das potentiell diskriminierende

[6] http://www.iata.org/whatwedo/security/Pages/smart-security.aspx; Die TSA verwaltet die sog. „No Fly-List". Aus den Programmen CAPPS 1 und 2 wurde Secure Flight. vgl. http://www.iata.org/pressroom/pr/Pages/2013-12-12-02.aspx. auch LII / Legal Information Institute (Hg.) (2014): 49 U.S. Code § 114 – Transportation Security Administration. Online verfügbar unter http://www.law.cornell.edu/uscode/text/49/114#h_2, zuletzt aktualisiert am 11.12.2014, zuletzt

Verfahren, das im so genannten 3-Tunnel-Modell besonders versinnbildlicht ist, ist nun allerdings nicht mehr vorgesehen. Stattdessen wird explizit betont, dass keine religiösen, ethnischen oder geschlechtsbezogenen Kriterien Grundlage der Differenzierung sein sollen: Vielmehr werden sozial und kulturell unverfängliche bzw. neutrale Aspekte betont, wie das zufällige Auswählen von Passagieren für intensivere Kontrollen. Soziale und kulturelle Differenzieren werden zudem stärker in technische Lösungen „eingebettet", Moral auch an nicht-menschliche Akteure, hier an technische Artefakte delegiert (Adey: 2004 vgl. auch Maguire 2014 zur Konstruktion von Normalität an Flughäfen, speziell an Sicherheitsschleusen). Dies ist insofern relevant, da das Augenmerk darauf gerichtet werden kann, wie soziale und moralische Aufgaben an technische Lösungen weitergegeben werden können und so eine argumentative Entlastung der sozialen Dimension möglich ist. Im Hinblick auf den *Checkpoint of the Future* ist dies insofern wichtig als an technische Lösungen delegiert werden sollen, etwa die Auswahl von strenger zu kontrollierenden Passagieren per Zufallsgenerator. Aber auch die „Biometric identification" als weiterer Maßnahmenbestandteil lässt sich in diesem Sinne als Delegation einer moralischen Verantwortung an eine Technologie verstehen. Gleichzeitig, so ließe sich folgern, verschleiert dieses Delegieren an technische Lösungen das kulturelle Differenzieren und Identifizieren, das trotzdem Bestandteil des *Checkpoint of the Future* bleibt. Für eine aus Sicht der IATA erfolgreiche Umsetzung ist es wohl entscheidend, einen sozial und kulturell diskriminierenden Gehalt auszuschließen. Gleichzeitig bleibt in letzter Konsequenz – auch mit dem Verweis auf den Zusammenhang von kultureller Identität und islamistischen Terrorismus – diese Problematik unausgesprochener und inhärenter Bestandteil der Passagierdifferenzierung.

Bereits genutzte und geplante Sicherheitsmaßnahmen, bei denen die Passagierdifferenzierung zum Kern gehört, sind auch vor dem Hintergrund von Diskriminierungserfahrungen kritisch zu sehen, die beim Fliegen aufgrund von sozialen oder kulturellen Zuschreibungen gemacht werden. Solche Erfahrungen lassen sich als kritischer Kommentar verstehen, da so die Effekte eines wie auch immer gearteten *social sorting* deutlich werden. Nach Auswertung der ersten Interviewphase (vgl. Herlyn & Zurawski 2015; auch Herlyn 2014) war auffällig, dass von Männern mit muslimischem Hintergrund explizit thematisiert wurde, dass sie aufgrund ihres kulturellen Hintergrunds schärfer kontrolliert würden. Im folgenden Ausschnitt ist es

---

geprüft am 05.01.2015. Vgl. auch: 108th Congress: Intelligence Reform and Terrorism Prevention Act, zuletzt geprüft am 05.01.2015; Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung für die Zwecke des Programms der USA zum Aufspüren der Finanzierung des Terrorismus(TFTP) (2009). Online verfügbar unter http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/de/jha/111563.pdf, zuletzt aktualisiert am 30.11.2009, zuletzt geprüft am 06.01.2015.

ein tunesischer 26-jähriger Arzt, der beschreibt, dass er im Vergleich mit seinen europäischen Kollegen eine Ungleichbehandlung erfährt, die er nachvollziehbarerweise auf seine arabischen Herkunft zurückführt.

> "So I travel a lot and I do a lot of exchange in airports, change airports (...) and what I have seen, everytime I go through a Western European country they look at Arabs differently. So it doesn´t matter if you have a green passport. (…) I have some friends and they are European, we travel together, but from all the people they just come to me because I´m an Arab and they take me away from the line and they start asking questions and they are looking at the passport. It´s understandable according to the circumstances but sometimes they overdo it you know."

In diesem und weiteren Interviews zeigte sich, dass es bei den Flugreisen jeweils einzelne Erlebnisse gab, in denen die Gesprächspartner sich aufgrund ihres kulturellen Hintergrunds diskriminiert fühlten, und diese für sie zu einem Gesamtbild einer kulturell begründeten Ungleichbehandlung führten. Dies war teilweise auch so, weil diese Erfahrungen mit anderen Alltagserfahrungen in Beziehung gesetzt wurden, wie im Beispiel gezeigt wird. Sicherheit am Flughafen ist aus diesem Blickwinkel kein rein normativer Wert an sich, die benutzten Technologien nicht neutral, noch können sie allein für sich bewertet werden. Erst wenn die Zusammenhänge zwischen Raum, Technologie, den Sicherheitspraxen sowie den handelnden Personen (Passagiere und Sicherheitspersonal) zusammengenommen betrachtet werden, entsteht ein differenziertes Bild, welches man als Raum Flughafen beschreiben kann – jenseits von Architektur, physischer Umwelt und den mutmaßlichen Objekten und politischen Zielen von Technologie.

In analytischer Hinsicht gewährt die Betrachtung von Flughäfen als Anwendungsfeld von Überwachung einen Blick in die Praktiken der Risikogesellschaft, in der – wie Beck festgestellt hat – der Ausnahme- zum Normalzustand zu werden droht (ebd. 1986, 105; auch Maguire 2014). In diesem Sinne plädiert Bonß (2011) auch für eine neue Kultur der Unsicherheit, in der selbige als Produktivitätsressource nutzbar gemacht werden kann. Das Bekenntnis zur Unsicherheit als Bezugspunkt menschlichen Lebens, so Bonß, erlaubt neue Perspektiven auf Gesellschaft und vorhandene Gefahren und Risiken. Die Sicherheit wäre nicht länger das Maß aller Dinge, sondern relativiert. Das nach wie vor praktizierte Ideal der absoluten Risikobeseitigung hat als ein Nebeneffekt nicht nur die beschleunigte Entwicklung zu immer mehr Sicherheit, die ausgrenzt, falsche Versprechungen macht und letztlich ihre eigenen Gefahren tatsächlich mit produziert oder hier diskursiv nachhelfen muss. Das Beispiel der Sicherheit an Flughäfen zeigt zudem an einem besonders markierten Feld, diese Entwicklungen, Verwicklungen und teilweise scheinbar unauflösbaren Dilemmata. Diese sind die Hintergründe für eine Bewertung möglicher Konsequenzen technischer Innovationen an Flughäfen im Kontext von

Überwachung, Kontrolle und Sicherheit, auf die ich weiter unten noch einmal zurückkommen werde.

4.3 Urbaner Raum und die smart cities

Städte bzw. städtischer Raum sind seit jeher Orte der Überwachung. Daran ändert auch der Umstand nichts, dass die Stadt einmal als Ort der Freiheit gesehen wurde, in dem die soziale Kontrolle des ländlichen Raumes, des Dorfes, nicht in gleicher Weise bestanden hatte. Städte, das zeigen historische Arbeiten (vgl. u.a. Clark 2009), waren immer umkämpfte Räume, in denen Deutungshoheiten und Macht ausgehandelt wurden. Somit waren sie wohl schon immer auch Ort von Überwachung, gleichermaßen von Raum und Personen (vgl. Coleman 2005). Am Beispiel der Straßenbeleuchtung macht Kammerer deutlich (vgl. ebd. 2008, 19ff), wie der Staat ab dem 17. Jh. dafür sorgte, dass die Sichtbarkeit des Raumes und somit auch der sich dort aufhaltenden Personen zu seinem Monopol wurde. Die Beleuchtung wurde zur Aufgabe und Hoheit der Stadtverwaltungen und ist es bis heute geblieben. Kammerers dann folgende Analyse greift dabei die technische Innovation auf, die mittlerweile zur bildhaften Verkörperung urbaner Überwachung geworden ist: die Videoüberwachung. Graham spricht bereits 2002 von den Kameras als der fünften urbanen Infrastruktur, neben Wasser, Gas, Elektrizität und Telekommunikation. Die Mischung aus räumlicher Überwachung, der Verfolgung von Personen und der mutmaßlichen präventiven Wirkung der Kameras im Hinblick auf die Begehung bzw. die Verhinderung von Verbrechen in der Öffentlichkeit, haben Kameras zu dem Mittel der Überwachung öffentlicher Räume gemacht. Dazu kommt, dass in Großbritannien seit Beginn der 1990er Jahre diese Technik einen derartigen Boom erlebte, dass Stadt und Kameras vor dem Hintergrund des Bildes unsicherer Städte in einer Risikogesellschaft zu einer gedanklichen Einheit wurden (vgl. zu einem Überblick über die Entwicklung und zum Forschungsstand hinsichtlich Kameras u.a. Armstrong & Norris 1999; Norris, McCahill & Wood 2004; Töpfer 2007; Webster et al. 2012; Zurawski 2014). Städte und urbaner Raum bieten als Anwendungsfeld von Überwachung vielfältige Möglichkeiten, die weit über Videokameras hinausgehen, und dabei oftmals tief in das Alltagsleben der Bewohner und Besucher eingreifen. Die Gründe dafür liegen in der Beschaffenheit von Städten selbst, aber auch in den Vorstellungen, die diese umgeben, in den Träumen, die auf sie projiziert werden und in der Bedeutung, die sie gegenwärtig und zukünftig politisch, sozial und wirtschaftlich spielen bzw. spielen werden. Mehr als 50% der Weltbevölkerung lebt in Städten[7], in Westeuropa und Amerika dürften es weitaus mehr sein. Die wirtschaftlichen und politischen Zentren sind urbane Agglomerationen, oftmals von einer Größe jenseits der Regierbarkeit und damit auch Orte der

[7] http://www.bundesregierung.de/Content/DE/Magazine/MagazinEntwicklungspolitik/068/s0-jahrtausend-der-staedte-bmz.html (7.11.2015)

Unsicherheit, der Ungleichheit, des Ausschlusses und des permanenten Risikos (vgl. zu Unsicherheit Koonings & Kruijt 2007; Wehrheim 2012; Häfele 2013; zu Ungleichheit Belina 2011a; LaGory & Fitzpatrick 2011; Berger et al. 2014; zu Risiko Belina 2011b und Dickson et al. 2012), z.B. von Terroranschlägen, Katastrophen, Unfällen oder von nicht mehr zu kontrollierenden Bevölkerungsgruppen, d.h. sie sind Orte eines Versagens des urbanen Managements hinsichtlich der Aufrechterhaltung eines Rechtsstaates. Dass die Ursachen und Effekte von Risiko und anschließenden Sicherheitsmaßnahmen durchaus verquickter und nicht linear sind, ist anzunehmen, kann hier aber nicht tiefergehend behandelt werden. Städte, so zahlreiche Analysen, sind nicht nur Orte des Fortschritts (was sie schon immer waren), sondern mittlerweile zu der bestimmenden Lebensform des 21. Jahrhunderts geworden, und damit verstärkt zu Orten des Risikos und somit zu Testlaboren der möglichen Gegenmaßnahmen in Form weiterer technischer Innovationen sowie in Form von Managementprozessen politischer und sozialer Art. Von einem militärischen Urbanismus spricht Graham 2010 (*new military urbanism*), als Ergebnis globaler Verstädterung und dem Umgang damit verbundener Probleme. Städte, so seine Analyse, würden sich im Krieg befinden, im Krieg gegen Terror, Drogen, Unsicherheit, Kriminalität. Technologie spielt in diesem Krieg eine entscheidende Rolle und führt bereits jetzt zu einer Militarisierung urbanen Lebens (ebd. 2010, xiiif, auch 60-88).

Jenseits der generellen Entwicklung von Städten zu Orten der Überwachung, wie sie verschiedentlich festgestellt wird, lässt sich der Raum Stadt als solcher in Ebenen einteilen, die zu einem Anwendungsfeld werden können. Der Raum von Städten, die Stadt als Raum (d.h. als Möglichkeit der Erfahrung und der Umsetzung technischer Innovationen) gliedert sich auf, wobei die Kategorien einer solchen Einteilung wiederum das Objekt von Aushandlung ist. Generell lässt sich das Anwendungsfeld im Hinblick auf eine Überwachung oder Kontrolle in folgende Bereiche unterteilen:

1. Öffentlicher Raum: Kriminalitätskontrolle, Kontrolle der öffentlichen Ordnung (Demonstrationen usw.), soziale Kontrolle, Überwachung von Verkehr, Management von Bewegungsströmen, Überwachung von Straßen, von Bewegung, Einlass und Restriktionen.

2. Nicht öffentlicher Raum: insgesamt schwierig zu überwachen ohne die Privatsphäre und Bürgerrechte zu verletzen, über die Infrastrukturen bieten sich hier Möglichkeiten. Aber auch über die Einrichtung von zivilgesellschaftlichen Kontroll- und Überwachungsmaßnahmen ist hier eine Überprüfung und die Kontrolle möglich, z.B. über die in manchen Ländern verbreitete Institution des Neighbourhood Watch (für. Großbritannien vgl. Bennett 2006; Bullock 2014, vgl. auch IRiSS-Bericht WP 3[8]).

[8] http://irissproject.eu/wp-content/uploads/2014/06/D3.2-Surveillance-Impact-report1.pdf1.pdf

3. Infrastrukturen der Stadt: Überwachung als Schutz vor Angriffen; Überwachung als Schutz der Bevölkerung vor Unfällen; Kontrolle der Aktivitäten der Bürger, aktiv im Verkehr, d.h. wieder im öffentlichen Raum, oder vermittelt über die Kontrolle der messbaren Ergebnisse ihrer Aktivitäten, wie Stromverbrauch, Internetnutzung usw..

Als eine zusätzliche Ebene kann die mittlerweile weit vorangeschrittene Vernetzung der Welt über das Internet angesehen werden. Das Stichwort des *Internet der Dinge* (Anderson 2013; Andelfinger 2014; Bessis & Dobre 2014) hat Einzug sowohl in die wissenschaftliche Diskussion, als auch in die populären Publikationen erhalten und hat Konsequenzen für urbane Räume auch im Hinblick auf deren Kontrolle und Überwachung. Ein Beispiel dafür mag die Debatte über so genannte *smart meters* sein, digitale und vernetzte Stromzähler (Hess & Coley 2012; Horne et al. 2014), mit denen man den Stromverbrauch effizient gestalten kann, aber damit auch gleichzeitig die Gewohnheiten der Nutzer ablesen und überwachen kann. Eine Steuerung des privaten, nicht-öffentlichen Bereiches wird hiermit möglich.

Die vernetzte Verbindung von Infrastrukturen und damit eine Kommunikation zwischen den „Dingen“ und den Menschen ist Teil des Urbanen geworden und somit auch ein Teil seiner Überwachung. Amin & Thrift (2002) Graham (2005), aber auch Kitchin & Dodge (2007) und Kitchin (2014) weisen darauf hin, wie über Software die sozialen und technischen Infrastrukturen urbaner Umwelten gesteuert werden. Städte sind geradezu abhängig von Code und Software. Software, technische Innovationen, Raum und das alltägliche Leben sind ineinander verwoben, bedingen sich gegenseitig und formen das Reservoir, aus dem sich Stadt heraus bildet, mit allen entsprechenden Möglichkeiten, Realitäten und Begrenzungen, die sich daraus ergeben.

> *With computerized systems now actually becoming the ‘ordinary’ sociotechnical world in many contemporary societies (Amin and Thrift, 2002), code orchestrates a widening array of public, private and public-private spheres and mobility, logistics and service systems and spaces. This new ‘calculative background that is currently coming into existence’, (...) is based on ubiquitous, pervasive, interlinked arrays of computerized spaces, systems and equipment which increasingly blend seamlessly into the wider urban environment.* (Graham 2005)

Hiermit wäre das verwirklicht, was Ericson &Haggerty (2000) mit einer *surveillance assemblage* gemeint hätten – nicht mehr das Panopticon als Gebäude, sondern die vernetzte Überwachung des Lebens, eingebaut in den Alltag und die Umwelt selbst. Und diese Entwicklung ist nicht nur theoretisch, sondern kann durchaus im Alltag beobachtet werden. Nicht zuletzt der Erfolg der Smartphones (und der damit verbundenen technischen Protokolle) hat dazu beigetragen, dass der Stadtraum mit neuen Kommunikationsebenen überzogen wurde: Navigationshilfen, Apps, die miteinander und mit dem „Raum“ kommunizieren, sei es im öffentlichen

Personennahverkehr oder mit Gebäuden und anderen Infrastrukturen (vgl. Meyer 2014, Jaekel & Bronnert 2013; Schulzki-Haddouti 2014)[9]. Verkehrskonzepte bauen schon heute auf solche Vernetzungen, wie das SwitchHH-Konzept in Hamburg zeigt, in dem Car-Sharing, der ÖPNV (U/-Bahnen) und das Leihfahrradsystem zusammengeschlossen wurden, und welches über Smartphones bedienbar ist. Und selbst das Auto, Inbegriff von Unabhängigkeit (vgl. Möser 2002; Volti 2006) und Freiheit, ist zunehmend Teil der *software sorted geographies* (vgl. Graham 2005), wenn es darum geht den Komfort des Fahrens mit den Anforderungen moderner Mobilitäts-, Versicherungs- und Kontrollkonzepte zu kombinieren, wie Schulzki-Haddouti in einem Überblicksartikel sehr eindrucksvoll herausgearbeitet hat (vgl. 2014).

Bezogen auf einzelne Aspekte zeigen z.B. die Arbeiten des SafetyLab des Fraunhofer Institutes (ein Forschungsprojekt des Fraunhofer Fokus Institutes[10]), dass die Anwendungen, an denen gegenwärtig gearbeitet wird, genau auf diese Vernetzung setzen, hier v.a. um Bürger in Notsituationen besser mit Informationen zu versorgen. Und diese können durchaus sinnvoll sein und einen echten Mehrwert für Bevölkerung und urbanes Management darstellen. Im Fall des SafetyLab geht es um ein besseres Katastrophenmanagement, letztlich also um eine verbesserte Sicherheit der Bürger durch Informationen. Weitergedacht geht es aber auch um das Management von Bevölkerungsströmen und urbaner Infrastruktur, Verkehr, Gebäuden etc., womit deutlich wird, dass der urbane Raum nicht nur über die „beleuchtete Sichtbarkeit", die Überschau, zum Anwendungsfeld von Überwachung wird, sondern sich die Kontrollen, Managementprozesse und Überwachung zu einem integralen Teil der Infrastruktur selbst entwickeln. Das, was im SafetyLab bezogen auf die Kommunikation in Katastrophenfällen erdacht wird, ist Teil weiter gehender Entwicklungen, die unter dem Begriff der *smart cities* zusammengefasst werden können. Smart Cities sind der Ausdruck der *software sorted geographies*, in denen eine Stadt in all ihren Aspekten effizient gemanagt werden soll (vgl. z.B. die IBM Werbevideos zu dem Thema[11]; vgl. auch Bourdin et al. 2014; Offenhuber & Ratti 2013; Jakubowski 2014; Kaczorowski 2014; Townsend 2014). Ob die darin beschrieben Computertechnologien zur Lösung urbaner Probleme weltweit die ideale Lösung sind, oder es sich vor allem um eine Wirtschaftsstrategie handelt, muss hier offen bleiben. Klar ist, dass damit die Stadt zu einem Anwendungsfeld von Überwachung durch technische Innovationen wird. Auch das SafetyLab spricht, im Zusammenhang mit seinen Vorschlägen zur technischen

[9] Vgl. Vernetzt und intelligent. Die Stadt der Zukunft? (2015). Online verfügbar unter http://future.arte.tv/de/thema/stadt-der-zukunft, zuletzt aktualisiert am 05.01.2015, zuletzt geprüft am 05.01.2015.

[10] In seinem safety lab bietet das Berliner Forschungsinstitut Fraunhofer FOKUS einen Demonstrationsraum, in dem das Zusammenspiel innovativer Technologien und effektiver Abläufe im Krisen- und Katastrophenmanagement simuliert werden kann.

[11] http://www.ibm.com/smartercities (10.1.2015)

Verbesserung der Kommunikationswege in der Stadt, von einem Prozess des „*making cities smart*“.

Vor diesem Hintergrund und angesichts der Tatsache, dass die globale Rate der Urbanisierung über 50 % beträgt und die Stadt auch darüber hinaus tonangebend für einen globalen Lebensstil und die Konsummuster weltweit ist (vgl. Clark 2004; Rolf 2006; Pacione 2009; Miles 2010), ist der urbane Raum, wie immer er ausgehandelt und mit welchen Bedeutungen er besetzt wird, eines der zentralen Felder technischer Innovationen. Hier überlappen sich nicht nur der öffentliche und private Raum. Hier werden gleichzeitig auch Bevölkerung und Infrastruktur gemanagt. Es bieten sich somit vielfältige Ansatzpunkte zur Kontrolle und Überwachung von Menschen (und eben deshalb auch so viele Fallstricke bei der Entwicklung von Technologie), denn die Stadt ist auch Schnittstelle von sozialer und technischer Umwelt gleichermaßen. Da diese Umwelten aber nicht nach strikten Kausalitäten geregelt sind und in sich jeweils das Potenzial für anderes, kontingentes und auch widerständiges Verhalten beinhalten, können nicht sich nicht alle Wünsche der Kontrolle so einfach technisch umsetzen lassen. Das Management einer Stadt und ihre Dynamik lassen sich deshalb nicht allein technisch kontrollieren und steuern.

Genau diese Dynamiken besser zu verstehen ist für eine gesellschaftliche Analyse von Überwachung und Kontrolle, aber auch generell für Gesellschaftsbetrachtungen, elementar. Umgekehrt gilt dieses auch für die Entwicklung von Technologien selbst, die eben nicht für einen neutralen, technisch steuerbaren Raum entwickelt werden, sondern für einen sozialen Raum.

4.4 Zusammenfassung: Raum, Technik und angewandte Problemlösung

Die beiden Beispiele von Anwendungsfeldern technischer Innovationen zu Steuerung, Kontrolle und Überwachung von Räumen, Menschen und Prozessen sind sehr unterschiedlich, und zeigen damit vor allem die Spannbreite räumlicher Kontexte. Ausgehend von der Prämisse, dass **Raum sozial konstruiert** ist, sich also eine Nutzung und die soziale Bedeutung nur sehr bedingt festlegen und kontrollieren lässt, können für den Zusammenhang von Raum, Überwachung und Technik ein paar grundsätzliche Aussagen festgehalten werden. Dabei ist zunächst zu berücksichtigen, dass wie an den Beispielen Flughafen und Stadt deutlich wurde, das Konzept Raum an sich von zentraler Bedeutung ist. Insbesondere sind die jeweiligen Eigenheiten von Raum und seiner Wahrnehmung zu berücksichtigen, wenn Technologie zur Überwachung von Raum und darin befindlichen Personen angewendet wird.

Ein **Flughafen** ist ein weitgehend **privatrechtlich** organisierter Raum, **geschlossen**, in seiner Funktion zumeist den technisch-bürokratischen Erfordernissen des Fliegens unterworfen – vom Einchecken, über die Personen- und Gepäckkontrolle, bis hin zum Sicherheitscheck der Flugzeuge selbst. Eine nahezu totale Kontrolle ist hier sowohl rechtlich als auch organisatorisch und architektonisch besser möglich als in der Stadt, im urbanen Raum. Allein die generelle Wahrnehmung des Fliegens als potenziell gefährlich bzw. die Notwendigkeit erhöhter Sicherheit (beim Fliegen selbst als auch drum herum), erhöht die generelle Akzeptanz technischer Maßnahmen, auch die der eigenen Überwachung. Auch wenn Reflexionen über die Sicherheitsmaßnahmen an Flughäfen stattfinden und Merkwürdigkeiten wie eine mutmaßliche Diskriminierung bestimmter Personen auffallen und in wissenschaftlichen Studien thematisiert werden, sind diese im normalen Betrieb eher bedeutungslos.

Anders der Raum Stadt, in dem öffentliche Überwachungsmaßnahmen eingehend diskutiert werden. Ja, diese selbst kann zum Ort des Protestes werden, ohne dass dieses unterbunden werden darf. **Stadt und urbaner Raum sind öffentlich, demokratisch und ausgehandelt.** Diese Aushandlungen durch Überwachung zu unterbinden weckt Widerstand. Die Steuerung von Personen und Infrastruktur in der Stadt ist ungleich der von Bewegungsströmen an Flughäfen. Das Konzept der *smart cities*, welches diese Management- und Prozessabläufe, die an Orten wie Flughäfen funktionieren, auf Städte übertragen will, gerät dabei schnell an seine Grenzen – sowohl technisch, als auch gesellschaftlich. Eine hierarchische Steuerung des öffentlichen Raumes ist nicht vorgesehen und bleibt – wenn angestrebt – nicht ohne Gegenrede. **Technologie muss sich seiner Anwendungsfelder bewusst sein**, den Raum kennen und sich entsprechend anpassen. Gerade im Bereich von Überwachungs- und Kontrolltechnologien kann es sonst zu unerwünschten Nebeneffekten kommen, die eine Technologie wirkungslos werden lassen. Technologie als angewandte Problemlösung für das Management von sozialen Räumen, deren Bedeutung sich auch aus der Nutzung und Aneignung der Bürger speist, ist zumindest problematisch, wenn eine solche Idee nicht sogar gänzlich von den falschen Prämissen ausgeht. So lässt sich **Terror am Flughafen** nicht durch Technik verhindern, schon gar nicht lassen sich die dahinterstehenden Probleme lösen. Aber für den begrenzten Raum Flughafen sind es effektive Mittel, um ein sicheres Flugerlebnis zu garantieren. Im **öffentlichen Raum lösen Kameras keine Kriminalitätsproblematik**, sondern erkennen nur mehr oder schrecken vereinzelt Täter ab. Eine Kriminalpolitik wird dadurch nicht ersetzt, die Probleme nicht durch Technik gelöst. **Die einfache Verbindung von Technik und sozialer Dynamik wird überschätzt** – es gibt keine Sozialmechanik. Technische Lösungen sind immer nur so gut, wie es der Anwendungskontext zulässt.

5. Technik und Überwachung – Konsequenzen und gesellschaftliche Wechselwirkungen

Technologie hat Konsequenzen – diese banale Feststellung lässt sich historisch mit vielen Beispielen belegen. Nicht nur, dass etwas schneller, höher, besser oder leichter funktioniert, also Konsequenzen im Sinn der Technologie selbst hat. Technologien haben auch soziale Konsequenzen und Implikationen. So verändert Technologie nicht nur den Bereich, für den sie eingesetzt worden sind, sondern u.U. auch weitere Teile und Aspekte von Gesellschaft. Die Eisenbahn hat den Transport großer Güter über weite Strecken ermöglicht, den Transport von Menschen und damit auch die Struktur von Gesellschaft verändert. Nationalstaaten wie wir sie kennen wurden denkbar, weil die neuen Verkehrsinfrastrukturen es möglich machten sich als Teil eines fest umrissenen Territoriums vorzustellen. Arbeitsverhältnisse haben sich geändert, weil anders produziert werden konnte, aber auch, weil Massen anders, schneller und weiträumiger mobilisiert werden konnten. Konsequenzen und Implikationen dieser Entwicklung in der Rückschau festzustellen ist allenfalls zum Streit zwischen Historikern geeignet, aber generell nicht allzu schwierig. Zu bewerten wie sich eine Technologie in Zukunft auswirken wird, ist weitaus schwieriger, wenn überhaupt annähernd exakt möglich. Dennoch lohnt es, sich darüber Gedanken zu machen, was passiert, wenn eine Technologie eingeführt wird – im vorliegenden Fall zur Erhöhung von Sicherheit oder zur Lösung eines Sicherheitsproblems d.h. zur Beseitigung einer tatsächlich bestehenden oder mutmaßlich so wahrgenommenen Unsicherheit oder eines Risikos. Dabei gibt es durchaus unterschiedliche Ansätze diese Vorrausschauen zu betreiben. Man kann versuchen abzuschätzen, was eine Technologie bewirkt, z.B. wenn man Körper-Scanner an Flughäfen aufstellt. Aus der Perspektive der Anwender kann man damit besser verbotene Gegenstände feststellen, eventuell den Durchlaufprozess optimieren. Diese Perspektive bleibt auf die Technologie selbst beschränkt und auf das was technisch möglich ist und es ist darüber hinaus noch abzuwägen wie dadurch andere Arbeitsabläufe beeinflusst werden können. Letztlich geht es hierbei um die Lösung des Problems selbst, wegen der die Technologie ursprünglich eingesetzt oder entwickelt wurde.

Es ließe sich aber auch darüber nachdenken, was passiert, wenn man eine solche Technik auf die Passagiere anwendet und eventuell auf Unverständnis, Abwehr oder Angst trifft oder auch auf das genaue Gegenteil. Wie nimmt die Öffentlichkeit diese Technologie war und wie diskutieren die Medien darüber (vgl. dazu z.B. Hirschberger 2015)? Die Anwendung von Technologie wird kritisch reflektiert und es wird versucht aus den Erfahrungen der Gegenwart und Vergangenheit zu extrapolieren, um entsprechende Aussagen und Einschätzungen zu machen. Testläufe, experimentelle Live-Versuche mit Technologien, können darüber eventuell Auskunft geben. Wenn hier

etwas über die Konsequenzen von Technik herausgefunden werden soll, dann geht diese Betrachtung von der Technik selbst aus.

5.1 Kritik der Szenarien in der Sicherheitsforschung

Es böte sich aber auch an anders an solche Zukunftsmodelle heranzugehen, nämlich vom Bedarf aus: *Was wäre wenn und was bräuchte ich, um dieser Situation zu begegnen?* Insbesondere die Sicherheitsforschung baut in ihren Ausschreibungen (siehe die Ausschreibungen beim BMBF; auch Steinmüller et al. 2010) auf diese Art der Szenarien, die auf eine Technologie von einer Situation her schließen wollen: *Wenn ich Sicherheitsproblem xy habe, wie kann ich darauf reagieren, um den gewünschten Zustand abc zu erreichen?* Das ist nicht unbedingt unproblematisch wie aus den Einlassungen zur Szenarien-basierten Forschung zu Sicherheit deutlich wird.

> *Ziel [der Orientierung der Sicherheitsforschung an Bedrohungsszenarien] ist es, verantwortliche Akteure auf das mögliche Eintreten einer bedrohlichen Situation vorzubereiten, indem ihnen ermöglicht wird, Eventualpläne aufzustellen und Vorbereitungs- bzw. Trainingsmaßnahmen zu ergreifen. In der Regel bestehen die Szenarien in der Darlegung der Bedrohungssituation als solcher. Zukünftige gesellschaftliche und politische Entwicklungen, die sich aus dem Handeln von Wissenschaft, Politik, Bedarfsträgern und Gesellschaft ergeben und die selbst wiederum von möglichen Ergebnissen der deutschen Sicherheitsforschung beeinflusst sein können, sind nicht Gegenstand der szenarioorientierten Betrachtung von „Sicherheit". An dieser Stelle setzt der Szenarioprozess des Forschungsforums Öffentliche Sicherheit mit dem Ziel an, eine zielgerichtete und fundierte Reflexion der politischen und wissenschaftlichen Praxis in der Sicherheitsforschung zu ermöglichen*. (Steinmüller & Gerhold 2010, 9).

Die eigentliche Crux von solchermaßen orientierter Forschung liegt demnach im Nachdenken über diese Szenarien selbst. Bevor ich in dieser Expertise über die Konsequenzen und Implikationen von Technologien im Kontext von Überwachung nachdenken möchte, sollen zunächst die Dimensionen von Szenarien als Ausgangspunkt technologischer Forschung erörtert werden. Denn bereits hier treten Probleme auf, die es sich durchaus zu reflektieren lohnt. So geht es beispielsweise in diesen Szenarien – im Unterschied zur direkten Abschätzung von möglichen Folgen eingeführter Technologien – darum, technische Lösungen und Anwendungen für Probleme zu finden, die nur in einem bestimmten Szenario gebraucht werden könnten. Das bedeutet auch, dass Technologien für Situationen erfunden und entwickelt werden, die real sein können, aber bei weitem nicht sein müssen – die eine Wirklichkeit vorwegnehmen, die sie eventuell selbst erzeugt haben. Dabei bleiben die von der Technologie ausgehenden Konsequenzen, die nur dann zu ergründen sind, wenn Technologie

nicht als Ding allein, sondern als Ding in einem Kontext gesehen wird, weiterhin bestehen.

Es geht bei diesen Szenarien, wie bei aller Zukunftsforschung wohl darum ein zukunftsbezogenes Orientierungswissen zu schaffen, um darauf basierend Entscheidungsmodelle zu entwickeln (vgl. Gerhold et al. 2015, 9). Dabei gilt es, so die Autoren, entwickelte Standards einzuhalten, um eine Zukunftsforschung zu betreiben, die eben nicht gänzlich im Reich der Fiktion angesiedelt ist.

> *Der Zukunftsforschung ist ein solcher Weg verschlossen. „Zukunftsspuren" in einem strengen Sinne gibt es nicht, allenfalls Fakten, die zukunftsbeeinflussendes Potenzial in sich tragen, deren weitere Entwicklung oder Wirkung aber grundsätzlich ungewiss ist. Zukunftsforschung unterscheidet sich von den „Vergangenheitswissenschaften" also dadurch, dass ihr Gegenstand weder ist noch war, sondern (möglicherweise) sein wird und daher die von ihr getroffenen Aussagen einer direkten empirischen Überprüfung vollständig entzogen sind – solange sie noch Zukunfts-Aussagen sind.*
>
> *Diese Eigenheiten des Gegenstandsbereiches zukünftiger Entwicklungen und Sachverhalte bringen im Hinblick auf den Forschungsprozess und auf die Reichweite der Forschungsergebnisse eine Reihe von Besonderheiten gegenüber vielen anderen wissenschaftlichen Tätigkeitsfeldern mit sich. Aufgrund der reflektierten und spezifischen Berücksichtigung dieser Besonderheiten vermag die Zukunftsforschung einen wesentlichen und spezifischen Erkenntnis- und Problemlösungsbeitrag innerhalb der Wissenschaften zu leisten. (Neuhaus & Steinmüller 2015, 17f.)*

Weiterhin halten die Autoren fest, dass es bei zukunftsbezogenen Aussagen um konstruierte Fakten geht und dieser Umstand durchaus reflektiert werden müsse, denn nur dann könne man,

> *dem spezifischen Gegenstandsbereich […] zum einen Rechnung [ge]tragen […], indem man zukunftsbezogene Aussagen konsequent als gemachte (konstruierte) Bilder einer kontingenten Zukunft oder, kurz, als Zukunftsbilder versteht und bezeichnet – und eben nicht als vorweggenommene Abbilder künftiger Tatsachen.*

Zukunftsforschung würde ihre Aussagen über Zukunft als wissenschaftlich konstruierte Bilder eines zukünftigen und deshalb nicht faktischen Gegenstandes verstehen, so die Autoren. Ein zukunftsforscherischerKonstruktionsprozess erfordere daher auch eine besondere Reflexion und Kontrolle, beginnend mit der Klärung des Bezugsproblems. Es soll daher prinzipiell über Zukunft und nicht über Gegenwart und Vergangenheit gesprochen werden.

Diese besondere Qualität kann für die Szenarien, die als Ausgangspunkt für viele Projekte und Ausschreibungen der Sicherheitsforschung genommen werden, nicht unbedingt festgestellt werden. Sicherheit bedeutet hier in der Regel eine Aufzählung von möglichen Gefahren, denen es zu begegnen gilt ... *Was wäre wenn?* Der drohende Ausnahmezustand wird als *worst case*-Szenario ausgemalt. Mit Technologien und politischen Strategien soll diesen dann begegnet werden. Es besteht jedoch die Gefahr, dass sich gemachte Gefahrenbilder verselbständigen und die in der Folge entwickelten Technologien – mitsamt ihrer Implikationen für Bürger und Gesellschaft – ihre Daseinsberechtigung gleichsam erst durch die eigene Existenz schaffen, sich quasi retrospektiv rechtfertigen durch ihr bereits-Vorhandensein als Antwort auf ein Problem, welches nun beseitigt werden könne. Anhand der Installation von Kameras in Hamburg wurde (vgl. Zurawski 2014) auf diese Begründungs-Schleife bereits schon einmal hingewiesen. Wo und ob Kameras hängen, ist von der Bewertung einer Situation abhängig. Räume werden als unsicher markiert, ein Umstand, der von den dann installierten Kameras bestärkt wird. Es ist dennoch fraglich, ob in Räumen, die durch Kameras als „unsicher" kategorisiert werden, Kameras letztlich auch zu einer Wiederherstellung eines beeinträchtigten Sicherheitsgefühl führen, wo sie doch durch ihre Präsenz zuallererst für jedermann deutlich eine Unsicherheit „konstruieren", zumindest aber diese sichtbar machen. Die Begründungen für eine Installation der Kameras werden den Beobachteten in Form von Sicherheits-/Unsicherheitsdiskursen und den darüber nach außen gedrungenen Vorannahmen oder Parametern der Überwachung vorgelegt. Die eigenen Erfahrungen oder Vorstellungen werden damit abgeglichen, die Argumente dann entsprechend in Einklang mit eigenen Bildern von der Welt gesetzt, angepasst oder verworfen. Auch hier kann es dann zu dem Phänomen kommen, dass die Kameras selbst als Grund ihrer eigenen Existenz an einem bestimmten Ort aufgefasst werden – etwa in folgender Logik: *...die Kameras hängen dort, weil sie gegen die Kriminalität installiert worden sind, auf die sie selbst noch einmal hinweisen bzw. deren Unsicherheitsdiskurs sie selbst erst hervorgerufen haben* ... (vgl. Zurawski 2014, 132ff.).

Diese Form von Szenarien ist jedoch die schlechteste Variante von Zukunftsvorstellungen, die bei näherer Betrachtung eigentlich gar keine Zukunftsprognosen sein sollen. Vielmehr geht es um so genannte Sicherheitsfantasien (vgl. Svenonius 2011, in diesem Fall basierend auf einer Vorstellung von Unsicherheit), die den schlimmsten Fall annehmen, um Mittel zu finden sein Eintreten zu verhindern. Diese Vorstellungen basieren zumeist auf bereits in der Gegenwart nur unzureichend gestützte Annahmen des Anderen, der Gefahr, die eine Sicherheit bedroht (vgl. auch Zurawski 2014c). Der Fokus auf Bedrohungsszenarien ist nicht unbedingt sinnvoll, bedarf aber dennoch einer näheren Betrachtung, um die möglichen Konsequenzen dieser Art von Vorstellungen zu skizzieren. Sinnvoller wäre es sicherlich Handlungs- oder Entwicklungsszenarien zu entwerfen, mit denen auch der Einsatz von Überwachungstechnologien reflektiert

werden kann. Das ist jedoch zumeist nicht der Fall. Es lohnt sich dennoch ein Blick auf diese Art von Bedrohungsszenarien, da man etwas über die gestellten Fragen erfährt und etwas darüber, welche Antworten man erwarten kann, also auch in welche Richtung eine Problemlösung tendieren soll. Überwachung ist in diesem Sinne Teil dieser Sicherheitsfantasien, in denen Szenarien als Wirklichkeitsmaschinen fungieren.

> *Today abstraction is no longer that of the map, the double, the mirror, or the concept. Simulation is no longer that of a territory, a referential being or substance. It is the generation by models of a real without origin or reality: A hyperreal. The territory no longer preceeds the map, nor does it survive it. It is nevertheless the map that proceeds the territory – precession of simulacra – that engenders the territory (Baudrillard 1994, 1).*

„Die Karte nimmt das Territorium vorweg“ – so lautet der Kern des Zitates des französischen Philosophen der Postmoderne und der Simulationen, Jean Baudrillard. Er nutzt zwar in dieser Argumentation geo- und kartographische Metaphern, bringt aber das Problem dennoch auf den Punkt. Simulationen, als die er auch Karten sieht, sind nicht mehr bezogen auf ein Territorium – eine materielle Wirklichkeit –, sondern werden selbst zur Referenz für alles, was darauf folgt. Analog zur Sicherheitsforschung, in der es weniger um Karten, aber ebenfalls um Bilder und Szenarien der Orientierung geht, lassen sich jedoch auch Vorstellungen finden, mit denen eine Wirklichkeit vorweg genommen wird. Zwar fehlen in der Sicherheitsforschung offen thematisierte räumliche und geographische Aspekte fast vollständig. Diese werden jedoch über die normativen Annahmen von Bedrohung, Gefährdung und (geo-politischen) Unsicherheitspotenzialen unterschwellig wieder in die Diskurse zurückgeführt. Baudrillards Zitat ergibt hier einen Sinn, wenn die Sicherheitsforschung als eine Forschung verstanden wird, die das Szenario als ein elementares Merkmal vieler Projekte entdeckt hat, welches in der Analyse nichts anderes als eine Simulation ist (vgl. de Lint 2008). Was bedeutet dieses aber für den Umgang mit Wirklichkeit, mit den tatsächlichen, mutmaßlichen, konstruierten oder erforschten Bedrohungssituationen oder Unsicherheitspotenzialen?

Szenarienbasierte Forschungen, wie sie als Grundlage der Sicherheitsforschung genommen werden, stützen sich auf Simulationen, die mithilfe in der Vergangenheit erhobener Daten und der Beobachtung von Phänomenen, die Zukunft neu interpretieren wollen. Es werden mögliche Ausnahmezustände ganz unterschiedlicher Art skizziert und es wird dazu aufgerufen sozio-technische Lösungen dafür zu finden. Das ist im Kern das Design vieler Projekte. Einzelne Programmlinien wie die „gesellschaftlichen Herausforderungen ziviler Sicherheit“ fallen nicht darunter, sind aber anschlussfähig. Der Bezug zur Gegenwart und Zukunft ergibt sich aus einer möglichen Wahrscheinlichkeit, der es mit einer Maßnahme dann zu begegnen gilt. Verkürzt lässt sich sagen, dass Szenarien auf gewisse Grundannahmen fußende Fantasien ihrer Urheber sind. Solche Szenarien sind insoweit Fiktion, als dass ihre empirischen Grundlagen

bestenfalls auf der Evaluation vergangener Ereignisse beruhen, schlechtestenfalls einfach nur einer Vorstellung des potenziell Möglichen entspringen – also eben nicht auf den Standards basieren, die Gerhold et al. (2015) für solche Arbeiten entwickelt haben. Im ersten Fall kann man von einer Verbesserung von Maßnahmen sprechen, im zweiten von der Konstruktion einer Wirklichkeit, wie sie grundsätzlich im Rahmen der Sicherheitsforschung als gegeben angenommen wird: Unsere Sicherheit ist in vielfältiger Weise bedroht, u.a. durch die Herausforderungen der Globalisierung und die durch sie entstandenen Vernetzungen und Abhängigkeiten weltweit.

Solche Simulationen sind generell nicht besonders neu. Die Versicherungswirtschaft benutzt sie, um eine Einschätzung der Eintrittswahrscheinlichkeit von durch sie versicherten Risiken zu gewinnen. Doch für eine Einschätzung von Autounfällen bestimmter Automarken im Zusammenhang mit einer bestimmten Alters- und Geschlechtsgruppe, sind die empirischen Daten wesentlich besser geeignet als für die Einschätzung eines Terror- oder Anschlagrisikos, zumal, wenn es sich dabei auch noch um den Ort oder die Art eines Anschlages oder eine ganz bestimmte Bevölkerungsgruppe handeln soll. Da dürften geheimdienstliche Tätigkeiten – bei aller Kritik – eine bessere Chance auf die Generierung von relevantem Wissen haben. Die Definition terroristischer Akte selbst steht einer tatsächlich brauchbaren Risikoeinschätzung im Weg, da sie zwar selten, vor allem aber plötzlich und dabei zeitlich und räumlich unvorhersehbar bleiben sollen (vgl. Nathanson 2010). Dass es bestimmte Muster von Anschlägen bei bestimmten Gruppen gibt und sich daraus Strategien ihrer Bekämpfung entwickeln lassen, zeigen Konflikte wie jene in Israel, Nordirland oder Kolumbien u.v.a.. Sie zeigen aber auch, dass die Veränderungen nicht monokausal sind, ein weites Feld gesellschaftlicher und politischer Akteure und Strategien umfassen und manchmal auch nur eine Verlagerung von Problemen, nie aber eine vollständige Beseitigung bewirken. Ob solche Veränderungen hauptsächlich technisch induziert sind oder die Technologie nur ein Abwehrmechanismus zur Bekämpfung von Symptomen ist, bleibt weitgehend unbeantwortet und wird auch nicht reflektiert. Und ob der Terror überhaupt (mit welchen Zielen auch immer) als das Sicherheitsrisiko unserer hoch-technischen Gesellschaften gelten kann, kann ebenfalls bezweifelt werden, wie Reichenbach (2010, 109) anmerkt. Terroristen, so Reichenbach, könnten nichts anstellen, was aus anderen Gründen nicht auch passieren könnte. Zu einem terroristischen Super-GAU, dem erfolgreichen Angriff auf ein Kernkraftwerk, und das hätten Fukushima und Tschernobyl gezeigt, kann es auch aus anderen Gründen kommen.

Nun kann man sich andererseits durchaus vorstellen, solche Risikokalkulationen auch für Anschläge auf Verkehrs- und Versorgungsinfrastrukturen u.ä. zu machen. Allein die empirische Datengrundlage für solche Wahrscheinlichkeiten ist dürftig, auch weil es kaum genug Anschläge in Europa gegeben hat, die ein eindeutiges Muster erkennen ließen. Dass es gerechtfertigt ist, diese Infrastrukturen und Institutionen zu schützen, ist

unwidersprochen. Es muss aber die Frage erlaubt sein, ob die genutzten Argumente zur Rechtfertigung von Industriemaßnahmen (Innovationen) und Veränderungen einer politischen Kultur zielführend sind, oder ob sie nicht viel mehr Dinge hervorrufen, die ohne diese Szenarien so nicht vorhanden wären?

Wenn die über solche Simulationen oder Szenarien konstruierten und in die Debatte geworfenen Hyper-Realitäten (Bogard 2006) zum tatsächlichen Maßstab der Dinge, zu einer vermeintlichen Wirklichkeit der Bedrohung werden, dann ist das zutiefst problematisch. Auch, weil immer weniger klar ist, **was Original und was Simulation** ist. Hier würde dann in der Tat die **„Karte das Territorium“** vorwegnehmen, ja gleichsam das Territorium sein. Eine Unterscheidung ist nicht mehr möglich (vgl. Bogard 2006, 70). Ein Schwerpunkt auf Szenarien-gesteuerter Forschung wird dann zu einem Problem, wenn über diese Szenarien und Simulationen Wirklichkeiten und Realitäten geschaffen werden, die sich vom Modell lösen und verselbständigen. Es werden selbsterfüllende Prophezeiungen geschaffen, die sich möglichen demokratischen Kontrollen, durch die Verlagerung in Expertengremien und Behörden, entziehen. Dies ist tatsächlich eine große Gefahr. So erzeugte und durch scheinbar wissenschaftliche Rationalität untermauerte Szenarien können auch dazu benutzt werden, politisch-demokratische Prozesse der Entscheidungsfindung über den Einsatz von sozio-technischen Verfahren auszuhebeln. Im Extremfall können solche Szenarien mit einem Eigenleben **zum permanenten Ausnahmezustand** mutieren, der eine Einschränkung von bürgerlichen Rechten und Freiheiten qua Forschung rechtfertigen würde bzw. dieses über neue Maßnahmen zum Schutze unserer Sicherheit einfach durch Implementierung von die Freiheit einschränkender Maßnahmen in weiten Teile unseres Alltages tut.

Es besteht auch bei der Reflexion über mögliche Konsequenzen technischer Innovation im Kontext von Überwachung und Kontrolle durchaus die Gefahr solche neuen Wirklichkeiten zu schaffen, gleichsam den Bedrohungsszenarien, in denen die Technologien ursächlich für alle Folgen verantwortlich wären. Auch hier gilt, wie bereits am Anfang und wiederholt festgestellt, dass technische Innovationen nicht aus sich selbst heraus für die Lösung gesellschaftlicher Probleme verantwortlich sind. Die technische Lösung sozialer Probleme ist so linear nicht vorhanden. Das bedeutet aber auch, dass Technologien nicht aus sich selbst heraus und durch das bloße Erscheinen oder ihre Anwendung gesellschaftlich problematische Folgen haben können. Dystopische Szenarien dieser Art sind wenig hilfreich den Kontext technischer Innovationen zu untersuchen und deren mögliche und weiterreichende sozialen, rechtlichen und ethischen Implikationen im Hinblick auf Überwachung zu analysieren.

5.2. Beispiele für Implikationen technischer Innovationen

Daher sollen an dieser Stelle ein paar Beispiele aus den beiden beschriebenen Anwendungsfeldern zeigen, welche möglichen Implikationen technische Anwendungen im Kontext von Sicherheit und Überwachung im Hinblick auf gesellschaftliche Dynamik haben können. Diese Beispiele sind dabei explizit nicht als Szenario konstruiert, sondern sollen eher als Anschauungsmodelle verstanden werden. Es geht dabei weniger um kausale Begründungs- oder Beweisketten, sondern eher darum, die durch die Einführung oder den Einsatz bestimmter Technologien berührten sozialen Dimensionen zu erörtern und Fragen zu formulieren. Der Nutzen von idealtypischen Handlungsmodellen oder vermeintlichen Kausalketten ist wenig hilfreich, wenn es in erster Linie darum geht die möglichen Tragweiten von Technologien einzuführen. Dann verbliebe man auf dem Niveau, das sich bei der Einführung von Kameras an einem beliebigen Ort beobachten lässt: Die Kameras können dann wahlweise Kriminalität reduzieren / Terror bekämpfen / Verhalten normieren oder stellen eine Bedrohung für die Privatsphäre dar. Hier werden entweder die Ziele mit den tatsächlichen Wirkungen verwechselt oder pauschal eine Kritik angebracht, die so nicht auf jede Kamera an jedem Ort zutreffen kann. Das gilt für andere Technologien analog ihrer Verwendung und ihres Anwendungsfeldes. Grundsätzlich wichtig für die Bewertung einer technischen Innovation innerhalb einer Überwachungsmaßnahme sind sowohl der soziale als auch der räumliche Kontext (siehe auch weiter oben), aber auch andere Aspekte verdienen eine Würdigung.

Um mögliche Konsequenzen von Technologien zu erörtern werden hier beispielhaft Fälle herangezogen, mit denen ein paar der Kernprobleme beleuchtet werden sollen, diese Beispiele sind wiederum: **Flughafen** einerseits und der urbane Raum andererseits. In zweitem werden die Implikationen und Wechselwirkungen anhand einzelner Aspekte diskutiert: **Stadionsicherheit** und **Megaevents**; **Bodycams**; **vernetze Stadt** und **urbanes Management**.

5.2.1 Beispiel Flughafen

Wie in der Darstellung der Anwendungsfelder bereits deutlich wurde, ist der Flughafen als Raum eher geschlossen, privatrechtlich organisiert und hat durch das Fliegen selbst eine hohe Affinität zu Technologie und Sicherheit (wenn auch zunächst vor allem in Bezug auf die Flugzeuge und das Fliegen selbst). Zusätzlich haben in der Geschichte der Flughäfen immer neue Wellen von Sicherheitsbedenken oder bürokratischen Erfordernissen dafür gesorgt, dass sich die Architektur und die Verfahren selbst weiterentwickelt haben. Neue Technologien wurden eingeführt, z.B. um sowohl das Gepäck als auch die Ladung zu durchleuchten, um vor Entführungen zu schützen oder um Anschlägen vorzubeugen, sowohl am Boden, wie auch in der Luft. So können

Terrorwarnungen oder eine allgemeine (Un)Sicherheitslage auch dazu führen, dass Passagiere bereits vor dem eigentlichen Flughafen, vor den Sicherheitschecks kontrolliert werden, nicht nur in Israel. Da ein Flughafen als Ort im Allgemeinen sehr zweckgebunden aufgesucht wird, sind die Implikationen von Technologie auf die weitere Gesellschaft eher begrenzt. Dennoch ist es nicht unbedeutend, wie Technologie hier eingesetzt wird, denn diese kann nicht nur die Passagiere selbst berühren, sondern auch weitere Personen, die nicht fliegen, aber Passagiere bringen oder abholen (in diesem Sinne Unbeteiligte), und das auch noch Jahre später angesichts der Speicher- und Verwendungsfristen. Auch lassen sich hier Trends erkennen, die an Flughäfen zunächst getestet werden, aber ihren Einsatz im Anschluss auch in anderen sozialen und räumlichen Zusammenhängen haben, z.B. öffentlichen Raum, in anderen Verkehrsmitteln oder in dem Flughafen ähnlichen Räumen, wie z.B. Stadien. Darüber hinaus sind Sicherheitstechnologien oder solche, die im Zusammenhang mit der Sicherheit rund ums Fliegen eingesetzt werden, nicht ausschließlich auf den Raum Flughafen selbst beschränkt. Verfahren zur Erfassung der Flugpassagierdaten, wie CAPPS I + II sowie deren Nachfolger Secure Flight[12], gehen in der Erfassung und vor allem der Speicherung von Daten darüber hinaus. Hier werden möglicherweise Rechte auf Datenschutz oder den Schutz von Informationen verletzt, was Auswirkungen weit über den Anlass der Speicherung selbst hinaus haben kann. Es könnten hier sowohl Mobilitätsprofile, als auch – in der möglichen Verbindung mit anderen Datenbanken – Konsum- und Gewohnheitsprofile erstellt werden. Auch wenn diese Art von technisch gestützten Verfahren für die Sicherheit im Bereich des globalen Flugverkehrs wichtig sein können, so berühren sie möglicherweise einen weiteren Personenkreis und definitiv andere Bereiche des persönlichen Lebens als den Flug als solchen.

In begrenztem Maße gilt es für jede technische Innovation zu prüfen, inwieweit hier Bereiche außerhalb des Flughafens selbst berührt werden, insbesondere, wenn es um die Erfassung von Daten geht, aber auch wenn diese Daten mit anderen Verfahren kombiniert werden, wie z.B. den biometrischen Merkmalen in Reisepässen. Sollten Querverweise über den Reisepass zu anderen Kontrollsituationen gemacht werden können, in denen z.B. Fluggastdaten abgefragt werden können, dann wäre das sowohl datenschutzrechtlich, als auch im Hinblick auf andere Freiheiten problematisch. Ob und wie diese Bereiche durch Verfahren der Datenabfrage und Speicherung berührt werden, lässt sich möglicherweise vor der Einführung mit so genannten Privacy Impact Assessments evaluieren (vgl. Wright & de Hert 2012; auch IRiSS Handbook 2014[13])

[12] http://www.tsa.gov/stakeholders/secure-flight-program (5.1.2015)

[13] http://irissproject.eu/?page_id=610, Handbook on increasing resilience in a surveillance society. Key considerations for policy-makers, regulators, consultancies, service providers, the media, civil society organisations and the public, 2014.

Abgesehen von Fragen des Datenschutzes, welcher vor allem im Zusammenhang mit der Identifikation von Passagieren und deren Zuordnung zu eventuell aufgestellten Kategorien der Bewertung wichtig ist, kommt der Passagier vor allem bei den Sicherheitskontrollen in Berührung mit Technologie. Kofferscanner, Torbögen oder Körperscanner sind die offensichtlichsten Techniken, neben den omnipräsenten Kameras, mit denen Flughäfen in aller Regel sehr umfassend überwacht werden. Die Konstitution des Raumes als sehr funktionell und stark zweckgebunden lassen nur extrem wenige Zweifel an der Berechtigung dieser Technologien aufkommen. Der „Körperscanner" (*Nacktscanner*), auch *security scanner* hatte in den Probephasen, z.B am Hamburger Flughafen zwischen 2010 und 2011, Diskussionen hervorgerufen, da hier vermutet wurde, dass Aspekte menschlicher Würde und des Datenschutzes verletzt werden könnten. Interessanterweise waren die Debatten zumeist darauf beschränkt und thematisierten nicht, ob der Einsatz sich arbeitspraktisch rechnen würde oder ob durch eine vermeintlich verbesserte „Durchsicht" der Passagiere der versprochene Zugewinn an Sicherheit eintreten würde. Auffällig war zu Beginn der Testphasen vor allem die hohe Fehlerrate der Technik, sodass Passagiere weiterhin auch von Hand kontrolliert werden mussten. Sollte die Technik eine effizientere Überprüfung der Passagiere zum Ziel gehabt haben, dann läge hier ein wesentliches Problem. Viel wichtiger als das tatsächliche Funktionieren der Technologie, welches sich mit neueren Generationen von Geräten mit Sicherheit verbessern wird, ist – und das gilt für fast alle technischen Innovationen im Bereich Flughafen – die Möglichkeit Passagiere hier an Technologie zur Überprüfung der Person (direkt über Scanner), der Mobilität und der Gewohnheiten (über Daten) zu gewöhnen. Die vermeintliche Unausweichlichkeit der Kontrollen und der nahtlosen Überwachung am Flughafen bedeutet den Erfolg eines Diskurses der Sicherheit, weniger der Technologie als solcher. Die Ausweitung der technologischen Unausweichlichkeit und die entsprechende Einrichtung des Raumes Flughafen erstreckt sich schon jetzt auch auf Bereiche, die nicht primär unter die Sicherheitsaspekte fallen, insbesondere den Bereich des Konsums, an Flughäfen also die Duty-free-shopping-Bereiche, welche in der Regel direkt nach dem Sicherheitscheck zwingend durchlaufen werden müssen, (vgl. Rekacewicz 2013). Technische Innovationen sind Träger von Diskursen, die eine Unvermeidlichkeit suggerieren. Über sie wird die Produktion von Sicherheit bzw. die vorher konstatierte Unsicherheit (durch Terror, Anschläge, Unruhe, abweichende Personen usw.) materialisiert. Nur wenn zwischen dem Reden über Sicherheit und den technischen Innovationen eine Übereinstimmung herrscht, kann eine hohe Akzeptanz für beide erreicht werden. Eine hohe Akzeptanz der Sicherheits-maßnahmen am Flughafen ist ja auch derzeit eher gegeben, zumindest dann, wenn man Akzeptanz nach Lucke (1995) als Resignation oder Ignoranz fasst. Eine Akzeptanz im Sinne eines i*nformed consen*t nach Lucke ist allein aufgrund der im Design angelegten Intransparenz von Sicherheitsmaßnahmen am Flughafen nicht vollständig möglich. Ein weiterer Aspekt diesbezüglich ist die Komplexität technischer Maßnahmen, die für Laien nur schwer nachzuvollziehen sein dürfte. Eine Akzeptanz im Sinne des *informed*

consent würde jedoch eine kritische Reflexion und daher auch ein umfängliches Wissen über die Akzeptanzobjekte voraussetzen (vgl. Bartl et al. 2014) Dass der Körperscanner abgelehnt wurde lässt ja noch keine Rückschlüsse auf die Bewertung der Gesamtheit der Sicherheitsmaßnahmen am Flughafen zu.

Eine Konsequenz daraus ist sicherlich auch, dass bestimmte Technologien durch diese Praktiken mit bestimmten Bildern von Sicherheit oder Unsicherheit aufgeladen werden. Taschenscanner in öffentlichen Gebäuden muten wahrscheinlich ungewöhnlich an, erinnern aber sofort an einen Flughafen, rufen das Bild von möglichem Risiko und der daran anschließenden Produktion von Sicherheit durch Technik hervor. Die Sicherheitsschranken, Taschenscanner und Ausweis- sowie Motivationskontrollen (*„Warum wollen Sie hierher, haben Sie eine Verabredung?“*) am Paul-Löbe-Haus in Berlin (dem Haus der Abgeordneten) sind für ein Gebäude eher ungewöhnlich, aber im Zusammenhang mit einem Diskurs der Sicherheit, in dem der Staat und seine Vertreter gefährdet sind, ergibt es nicht nur Sinn, sondern auch sofortige Akzeptanz. Ob es gesellschaftlich richtig und klug ist, dass sich gewählte Abgeordnete vor dem Bürger in dieser Art und Weise schützen (müssen), muss hier offen bleiben, ist aber durchaus eine Frage nach dem daraus resultierenden Bild und dem Verhältnis zwischen den beiden Gruppen wert. Abgesehen von der besonderen Bedeutung dieses Gebäudes, begegnen einem solche Kontrollen, die an die an Flughäfen selbstverständlichen Checks erinnern, vielerorts, vor allem dort, wo sie eher unerwartet sind, z.B. in Behörden, Stadien, Konzerthallen etc..

Die von Schlepper et al. (2015) festgestellten Flughafen-Analogien im Bereich der Schifffahrt, insbesondere dem Fährverkehr, zeigen Übertragungsmuster in einem Bereich, der dem Fliegen strukturell ähnlich scheint. Allerdings zeigen sie auch deren Begrenzungen, wenn es z.B. um eine durch Sicherheit bedrohte Wirtschaftlichkeit geht. Hier gibt es auf bestimmten Routen einfach Konkurrenzsituationen zwischen Schiff und Straße, sodass die wünschenswerten Kontrollen gar nicht entsprechend durchgeführt werden können ohne die Wettbewerbsfähigkeit zu gefährden. Da allerdings auch keine Anschläge auf Fähren bekannt sind, zumindest nicht in Europa, scheinen zunächst diese Risiken auch nicht in gleicher Weise zu bestehen.

Umso katastrophaler ist dann der Befund, dass die Sicherheitskontrollen an den Flughäfen doch nicht so sicher sind, wie die Betreiber geglaubt oder vorgegeben haben zu glauben. Im Gegenteil. Die Enthüllungen verdeckter Tester kurz vor Weihnachten 2014 haben das Vertrauen eher erschüttert und werfen die Frage auf, wie sich die intensiven Eingriffe in die Privatsphäre angesichts dieser Lücken überhaupt rechtfertigen lassen[14]. Oder, ob das Sicherheitstheater, welches veranstaltet wird, nicht genau nur das

[14] vgl. z.B.

ist: eine Aufführung um das subjektive Sicherheitsgefühl zu stärken, aber nicht notwendigerweise die Sicherheitsstandards selbst. Andererseits lassen die festgestellten Lücken auch danach fragen, ob die immer wieder hervorgerufenen Drohpotenziale und angeblich so hohen Risiken durch Anschläge denn tatsächlich gegeben sind – denn passiert ist ja nichts! Diese Frage lässt sich leider nicht zufriedenstellend beantworten, weil es bedeuten würde, es darauf ankommen zu lassen. Ein kruder Vorteil, der den Befürwortern von immer mehr Einschränkungen und der verbesserten Überwachung durch immer neue Techniken in die Hände spielt. Dass dies vor allem ein praktischer Vorteil ist, der weder durch Fakten noch empirische Erkenntnisse gesichert ist, sollte dennoch nicht vergessen werden.

Ob also die bestehende Sicherheit am Flughafen durch eine bestimmte Technologie bzw. durch ein Zusammenspiel verschiedener Verfahren (technisch, prozesshaft oder auch bürokratisch) erreicht wird, oder ob bestimmte Risiken einfach nicht vorhanden sind, lässt sich in vivo schlecht ermessen. Auch, weil es sich hier um ein ethisch problematisches Experiment handeln würde, das ungefragt mit den Passagieren durchgeführt würde. Die Einführung zusätzlicher Technologien kann also leicht mit dem Argument nach mehr Sicherheit verbunden werden, während die Abschaffung deutlich schwieriger wird, da es u.U. zu einem Weniger an Sicherheit beitragen könnte. Da der Beweis eines Zusammenhanges schwer ist, würde die Reduktion bestimmter technischer Maßnahmen, insbesondere an Flughäfen auf argumentative Probleme stoßen. Die Implikation davon wäre, dass Technik zur Produktion von Sicherheit immer eingeführt werden kann, und somit zu einer Gewöhnung auch an den Zustand der potenziellen Gefahr bzw. des Risikos beitragen würde. Hier ist nicht die Technik selbst Ursache dieser Konsequenzen, sondern die Technik als Träger von Bedeutung und der Botschaft von Sicherheit an sich. Aus diesen ersten Ausführungen lassen sich einige Fragen generieren, die auch für die Bewertung von Technologien im Kontext von Sicherheit und Überwachung zentral sind.

- Sind technische Innovationen eine Reaktion auf konkrete Vorkommnisse (und bestehende Probleme), die mit bisherigen Mitteln nicht gelöst werden können? Geht es also um Verbesserungen bisheriger Verfahren?

- Wo sind Konsequenzen und Implikationen von Technologien zu suchen? Im Bereich der Technologie selbst, ihrer Anwendung oder in ihrer symbolischen Bedeutung, die sich eben nicht auf den ersten Blick erschließen lässt?

---

http://www.hr-online.de/website/rubriken/nachrichten/indexhessen34938.jsp?rubrik=36082&key=standard_document_53917775

- Erreicht die Einführung von Technologien ihre eigentlichen Ziele? Und: Liegen diese Ziele im Rahmen der Technologie selbst oder in den mittelbaren Zielen, also verbesserte Überprüfung Einzelner vs. Verhinderung des Terrors?

- In welchem Bereich haben Technologien Folgen? Und wen betreffen sie? Die für (oder gegen) die sie installiert worden sind (z.B. die Passagiere)? Oder beim Betriebspersonal? Ändern sich dadurch z.B. Arbeitsabläufe und organisatorische Bedingungen für das Sicherheitspersonal?

- Um die Folgen von Technologie zu erforschen, bedarf es mehr als bloßer Umfragen, sondern qualitativer Studien sowohl bei den Passagieren, als auch beim Personal über Fragen der Wahrnehmung, der Arbeitsabläufe, oder ganzer Ethnographien zum Fliegen (vgl. z.B. Schaefer 2015) usw..

Durch den speziellen Raum des Flughafens ist anzunehmen, dass die direkten Konsequenzen von Technologie auf die Passagiere eher gering sind, auch wenn diese Akzeptanz darauf baut, dass die Alternative bedeutet nicht fliegen zu können. Unerwähnt blieb bisher die Frage nach den Konsequenzen eingeführter Technologien auf die Bediensteten selbst. Auch hier ist davon auszugehen, dass sich Arbeitsabläufe, organisatorische Bedingungen und die Wahrnehmung des Passagiers aus der Perspektive des Sicherheitspersonals verändert (dazu vgl. z.B. Rieger 2015; auch Bartl et al. 2014).

5.2.2 Beispiel Stadien und Mega-Events

Generell gilt für den öffentlichen, urbanen Raum, was auch im Anwendungsfeld Flughafen erörtert wurde: Technologie ist mit Bedeutung aufgeladen, dient als Projektionsfläche für Politik und ist eng an die Form der Sicherheitsdiskurse gebunden, die eine Einführung von Technologien zwangsläufig umgibt. Technische Ziele dürfen nicht mit den politischen und sicherheitspraktischen Zielen verwechselt werden. Folgen und Konsequenzen sind deshalb auch dort zu suchen, wo Technologie nur mittelbar über Bedeutung oder als Symbol wirkt. Anders als ein Flughafen ist eine Stadt offen. Die meisten Handlungen sind nicht aufeinander bezogen, das „Ergebnis“ (wenn es denn so etwas gibt) ist weitgehend unbekannt und kontingent. Die Stadt funktioniert, wie gezeigt, auf verschiedenen Ebenen, die einander bedingen, aber in der Wahrnehmung nicht unbedingt als logisch verbunden erscheinen, z.B. das Leben in einem Viertel und die unter der Straße verlaufende Infrastruktur die vor allem dann auffallen würde, wenn sie nicht verfügbar oder gestört wäre. Die Überwachung einer Stadt betrifft zumeist das Leben im öffentlichen Raum, wobei über eine Steuerung der Infrastruktur zunehmend auf den privaten Raum zugegriffen wird. An öffentlichen Orten, Gebäuden, Verkehr und Verkehrsinfrastrukturen werden Überwachungstechnologien, die im Rahmen einer wie auch immer definierten Sicherheit eingesetzt werden, maßgeblich angewendet,.

Angesichts der Vielschichtigkeit von Städten und der oftmals ambivalenten Bedeutung und Nutzung von Räumen, ist weder eine Aufzählung von Bereichen, noch von möglichst kategorisch geordneten Implikationen oder Konsequenzen so leicht möglich. Ein Bereich, der dem Flughafen relativ ähnlich ist – insbesondere von den Möglichkeiten den Raum zu kontrollieren und zu überwachen – sind Fußballstadien: Beides sind umgrenzte Räume, Gebäude, sehr zweckgebunden. Es sind viele Menschen auf einmal anwesend, die entsprechend gemanagt werden müssen. Aber da hören die Gemeinsamkeiten auch schon auf. Stadien ziehen in der Regel ihre Zuschauer in Massen auf einmal an. Die Zufahrt ist über den öffentlichen Raum (wie bei Flughäfen auch), aber eben nicht einzeln und kontinuierlich, sondern massenhaft und zu einem bestimmten Zeitpunkt. Das bedeutet, dass hier viele Menschen gemanagt werden müssen, dazu der Verkehr, eventuelles Aufeinandertreffen verschiedener Fangruppen, die möglicherweise aufeinander losgehen. Kameras im Stadion können hier nicht wirken. Mobile Kamerateams der Polizei, wie sie bereits eingesetzt werden, haben mehr eine dokumentarische Funktion, als dass sie Teil des Kontrollprozesses des Besuches selbst sind. Die Eingangskontrollen – mittlerweile mit Scannern ausgestattet –, ermöglichen in einem gewissen Rahmen eine Generierung von Informationen über die anwesenden Zuschauer. Da ein eingehender Check zeitlich und organisatorisch nicht durchzuführen ist, ist eine Identifizierung jedes Zuschauers da weder praktikabel noch erwünscht. Aspekte des Datenschutzes und des Rechtes auf Anonymität in der Öffentlichkeit könnten hier eine Rolle spielen, wenn letzteres auch eher eingeschränkt. Auch wenn der Besuch eines Stadions zu einem Fußballspiel auf den ersten Blick eine klare Intention hat – ein Fußballspiel zu sehen – so ist das Verhalten im Gegensatz zum Flughafen vollkommen ungeplant, oft spontan und kann nur sehr begrenzt durch weitere Kontrollen oder Überwachungstechnologie eingeschränkt bzw. gemanagt werden. Fangruppen entfalten Botschaften, politische, soziale und sonstige, engagieren sich in so genannten Choreographien, die sich auch gegen die Polizei, den Staat, den eigenen oder den gegnerischen Verein richten können. Technologien zum Zwecke der Überwachung können Opposition hervorrufen, oder aber, wie in Großbritannien geschehen (Giulianotti 2011; Spaaij 2013; Stott et al. 2012) zu einer Veränderung der Fankultur in den Stadien führen. Die Abschaffung von Stehplätzen, Sicherheitskontrollen, eine Veränderung der Architektur sowie des Preisgefüges der Tickets hat die berüchtigten Hooligans der 1980er fast vollständig aus den Stadien der oberen Klassen verschwinden lassen. Eine Versicherheitlichung von Fußball- und Stadionkultur war die wohl intendierte Folge dieser Maßnahmen mit dem Effekt eines tiefgreifenden Strukturwandels im britischen Fußball. Ähnliche Tendenzen sind auch in Deutschland feststellbar, treffen aber noch auf den Widerstand der Fans und Vereine.

Im Zusammenhang mit so genannten Mega-Events wie einer Fußball Weltmeisterschaft oder Olympischen Spielen lässt sich beobachten, dass die Sicherheit, die sonst nur unmittelbar um und in den Stadien herrscht, nun auf größere urbane Bereiche

ausgeweitet wird. Überwachung und Kontrolle finden überall statt. Der öffentliche Raum wird beschnitten und Bürger in ihren Rechten eingeschränkt, z.B. im Demonstrationsrecht (Haggerty & Bennett 2012; Klauser & Giulianotti 2012; Klauser & Fussey 2014). Entscheidend ist auch hier weniger die Technologie als solche, von der in diesem Sinne keine direkten Effekte ausgehen. Vielmehr ist sie hier Teil eines größeren Zusammenhanges, in dem allerdings die Definition von Räumen umkämpft ist, und das durchaus mit negativen Folgen für die Bevölkerung. Weiterhin kann der Einsatz von Technologie in Stadien auch für die Betreiber und das Sicherheitspersonal eine erhöhte Erwartung an die Umsetzung von normativen Vorgaben bedeuten, z.B. durch Sponsoren oder Verbände, die mit entsprechenden Wünschen an die Vereine und Veranstalter herantreten. Auch hier ist Technologie vor allem Träger von Bedeutung und Projektionsfläche von dem, was Svenonius (2011) mit **Sicherheitsfantasie** beschreibt.

5.2.3 Beispiel Bodycams

Während es im Beispiel der Stadien um ein ziemlich breit gefächertes Feld geht, handelt es sich bei der möglichen Einführung von so genannten Bodycams um eine recht konkrete Technologie, die in einem eng umrissenen Feld eingesetzt wird. Bodycams sind auf der Schulter montierte Kameras, die von Polizisten auf Streife im Einsatz getragen werden. Eingesetzt werden sie in den USA, von wo es auch erste Studien zur Effektivität und zu den möglichen Folgen gibt[15]. In Deutschland gibt es einen Modellversuch in Hessen, weitere in Hamburg und Nordrhein-Westfalen sollen eventuell folgen. Die parlamentarische Diskussion findet statt (Stand: Dezember 2014). Bodycams sind eine Technologie, eingesetzt im öffentlichen Raum, mobil und auf das polizeiliche Gegenüber in einer Kontaktsituation gerichtet. Das konstatierte Ziel ist die Prävention von Gewalt gegenüber Polizeibeamten, aber auch die Beweissicherung bei eventuellen Vorfällen. Abgesehen von den Problemen der gesetzlichen Verankerung dieser beiden Ziele, wird dadurch auch unklar worum es eigentlich wirklich gehen soll – und vor allem ob und wie diese Kameras einen präventiven Charakter haben sollen. Die Zahlen zum Feldversuch in Hessen sind dürftig und geben wenig Auskunft über die Effektivität dieser Technologie. Die Evaluation ist ungenügend, die Zahlen missverständlich, die Parameter nicht transparent und die erhobenen Zahlen für eine aussagekräftige Statistik nicht ausreichend. In der Darstellung des Versuches wird u.a. deutlich, dass insbesondere nachts und durch betrunkene Personen Angriffe auf

[15] http://www.policefoundation.org/content/body-worn-cameras-police-use-force; Justin Ready (o. Jahr): The Impact of on-office video cameras on police-citizen contacts: Findings from a Mesa field experiment. Arizona State University, vgl. u.a. hier: http://www.slate.com/articles/technology/future_tense/2014/09/ferguson_body_cams_myths_about_police_body_worn_recorders.html.

Polizeibeamte verantwortet werden. Affekttaten sind aber eher nicht präventiv zu verhindern, wie auch die Literatur zu Videoüberwachung ganz allgemein gezeigt hat.

Interessant an der Diskussion über die Einführung von Bodycams ist eine wohl eher nicht intendierte Folge. Argumente für diese Form der Kameras verweisen u.a. auf die USA und den dort erfolgreichen und bereits seit längerem bestehenden Einsatz dieser Technologie. Dabei wird von Seiten der Befürworter (Politik und Polizei) übersehen, dass eines der Argumente für die Kameras, die Überwachung und Kontrolle der Beamte selbst ist. Bodycams, so folgert die *American Civil Liberties Union* (ACLU) in einem Gutachten könnten ein Mittel sein, Polizeiarbeit zu dokumentieren (also Vorwürfe **gegen** die Polizei zu entkräften oder die Polizei selbst maßzuregeln) und gleichzeitig die Polizei zu schützen. Allerdings, so der Bericht der ACLU, nur dann, wenn es entsprechende Benutzungsregeln gibt und diese eingehalten und überprüft werden können. Bodycams dürften dabei nicht zu einer weiteren "normalen" Überwachung des Alltages durch die Polizei werden (vgl. dazu die Empfehlungen der ACLU[16]). Auch nach den Unruhen in Ferguson wurde eine Forderung nach Bodycams laut, als vertrauensbildende Maßnahme und Kontrolle der Polizei. Ob auf deutschen Straßen ähnliche Verhältnisse herrschen wie in New York, Los Angeles oder in Ferguson ist durchaus fraglich, aber eine Einführung dieser Technologie könnte das Vertrauen zwischen Polizei und Bürgern durchaus stören, wenn nicht klar ist, wie mit den Aufnahmen umgegangen wird, und ob es sich nicht nur um eine weitere Einschränkung des privaten Raumes durch die Polizei handeln könnte. Kritiker wie Briken & Eick (2013) würden eine solche Entwicklung mit der ohnehin zunehmenden Militarisierung von Polizei und der Kontrolle des öffentlichen Raumes zusammenbringen. Somit dient Technologie hier dazu Vertrauen herzustellen, hat aber gleichzeitig das Potenzial dieses Vertrauen ebenso nachhaltig zu stören. Technologie ist hier ein Vermittler, der gleichermaßen auf das Verhalten von Bürgern, als auch auf den Arbeitsalltag von Polizisten Einfluss haben kann und darüber hinaus auf das Verhältnis zwischen beiden.

Elementar bei der Bewertung einer solchen Technologie ist, dass die technische Innovation nicht als Lösung sozialer Probleme verstanden wird, sondern nur ein Mittler, ein Instrument ist, über das andere Aspekte ermöglicht werden können. Und ebenso wichtig ist es grundsätzlich zu verstehen, dass Technologien Nebeneffekte haben können, im Falle der Kameras die mögliche Überwachung der PolizistInnen im Einsatz selbst. Die Nutzung und Bedeutung der Kameras hängt auch von den sich herausbildenden Praktiken und projizierten Bedeutungen ab. Wird das nicht berücksichtigt und Technologie als Lösung von Problemen verstanden, bleiben Konflikte und Enttäuschen nicht aus.

[16]https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all (5.1.2015)

5.2.4 Beispiel vernetze Stadt und urbanes Management in der smart city

Handelt es sich bei den beiden vorherigen Beispielen um bereits bestehende Technologien, die zum Teil Realität sind, so sind die vielfältigen technischen Innovationen hinsichtlich eines urbanen Managements, der vernetzten Kontrolle der *smart city*, oft nicht mehr als aufwendige Werbekampagnen oder bislang vereinzelt existierende Technologien, deren totale Vernetzung noch auf sich warten lässt. Dennoch lohnt es sich einen Blick auf diese Idee zu werfen, um fragend abschätzen zu können, welche Implikation eine Umsetzung dieser Ideen habe könnte. Neben der Kontrolle der Infrastruktur – Energie, Verkehr, Versorgungsketten, Kommunikation – ist ein weiteres Ziel die Bevölkerung selbst. Dank einer zumindest in vielen Teilen Europas und der weiteren westlichen Welt mehr oder weniger vollständig digitalisierten Gesellschaft, ist die Überwachung, die Beteiligung als auch die Steuerung der Bevölkerung nur eine Frage der Anwendung und der Vernetzung und durchaus umsetzbar. Aber nicht nur die städtische Infrastruktur hängt an den digitalen Netzen und ist darüber Teil einer umfassenden, mittlerweile eben auch digitalen Sicherheitsarchitektur, sondern auch der Alltag an sich. In populären Artikeln mit Titeln wie „Dein Haus kennt Dich“ (Bachmann 2014) werden die Dimensionen und Implikationen der Verbreitung dieser Vernetzung ausgelotet. Als problematisch herausgestellt wird vor allem, dass bei jeder Gelegenheit und von jeder Tätigkeit Daten erhoben werden – nicht nur im Haushalt, sondern auch bei anderen Gelegenheiten. Schulzki-Haddouti (2014) hat wie auch Kitchin (2013) auf die Implikation der Einbettung von so genannten smarten Steuerungs- und Kommunikationstechnologien in Autos und weiter in die Verkehrsinfrastruktur hingewiesen. Von dem Auto, das mit dem Fahrer (der Fahrerin) spricht, über die Kommunikation mit der Werkstatt oder der Versicherung bis hin zum selbststeuernden Auto entfalten sich die Ideen der smarten Technologien rund ums Auto. Immer unter der Prämisse der Effizienz, der Sicherheit, aber auch der Kontrolle und letztlich der Überwachung. Warum allerdings der Spaß am Auto fahren gegen ein selbst fahrendes Auto eingetauscht werden soll, ein Auto also nur ein technisches Ding ist, und nicht ein Träger vielfältiger Bedeutung, Projektionen, ein Distinktionsmerkmal und ein Mittel der Identifikation, wird damit nicht beantwortet und ist ein festzustellender Mangel solcher Konzepte. Hier geht es um Technik der Technik willen – ganz entgegen jeder Autowerbung, die Freiheit, Spaß und ein Lebensgefühl vermitteln will.

Insgesamt geht es beim Konzept der *smart cities* um die informationstechnische und kommunikative Vernetzung von Technologien, die unterschiedliche Bereiche abdecken wie die private Kommunikation, den öffentlichen Verkehr, städtische Infrastruktur, persönliche und öffentliche Mobilität, Haustechnik, Energieversorgung, Konsumgewohnheiten, bis hin zur Wahrnehmung des urbanen Raumes (z.B. über Anwendungen, die mit dem Stichwort *augmented reality* verbunden sind (vgl. Guennon et al. 2008; Graham et al. 2012; Filonenko et al. 2014) und seiner informationstechnischen

Einbettung. Bei dieser Vernetzung kann man die Probleme der Datenerhebung, Verwendung und des Schutzes der Informationen und der angemessenen Datenflüsse bemängeln. Das hieße aber auch, dass als Lösung eine rein technische vorgeschlagen würde, nämlich den Einbau von Datenschutz in die Technik oder ihre Handhabung, und, dass sich über weitere Implikationen keine Gedanken gemacht werden muss. Der Fokus auf Datenschutz verhindert in diesem Fall eher das Nachdenken, als dass er eine adäquate Lösung bereitstellt.

Da diese Vernetzung zu einem großen Teil an den Alltagsgewohnheiten der Bürger ansetzt bzw. diese als Anschlusspunkt nutzt, ließe sich hier auch von einem Konsum der Überwachung sprechen (vgl. Monahan 2011; Zurawski 2011und 2014). Nicht alles, nur manches ist dabei bedeutend für die zivile Sicherheit, doch als Konglomerat verschiedener Technologien, gesehen als ein System, könnten die Implikationen wesentlich weiter gehen, als bloß die unachtsame Verwendung von Daten. Vielmehr werden mit den verwendeten Standards, den Diskursen von Nützlichkeit, Effizienz und dem „guten“ Leben Normen gesetzt, die neue Kontrollen und Überwachung überhaupt erst nötig machen. Zivile Sicherheit könnte durch die durchgeplante Steuerung der Bürger sowohl im privaten als auch im öffentlichen Raum stattfinden, auch weil man die Aktivitäten in beiden Bereichen aufeinander abgestimmt kontrollieren und steuern könnte. Es könnten Menschen-Ansammlungen verhindert werden und es müsste mit ihnen nicht umgegangen werden; Katastrophen könnten bei einer genauen Abstimmung bereits im Vorwege gemanagt werden; Bewegungen der Bürger könnten mit ihren Wünschen in Übereinstimmung gebracht werden, das Verhalten würde standardisiert, Überraschungen kontrolliert. Zivile Sicherheit würde bedeuten möglichst viele Unsicherheiten bereits im Vorwege durch eine umfassende Steuerung auszuschalten, so dass Kontrollen und Überprüfungen im Nachhinein gar nicht mehr nötig würden. Der Schlüssel dazu liegt in der Vernetzung von Lebenswelten, Technik, privater und öffentlicher Sphäre sowie dem Zugriff auf die Gewohnheiten der Bürger. Dass die Gesellschaft dabei mitmacht, sich quasi als Ausdruck des Konsums konform verhält und diese Entwicklung hin zum Guten und Praktischen, der Effizienz als solcher mitmacht, ist dabei entscheidend. Eine Welt, in der Gesellschaft den Erfordernissen der Ingenieure und Techniker folgt und Technologie zum Leitmedium wird, nicht länger ihre Bedeutung und der Umgang damit. Verdacht würde alles erregen, dass sich gegen diese Logik stellen würde. Es geht eben nicht um Datenschutz, sondern um neue Normen und ein neues Gesellschaftsbild, in dem die Szenarien nicht mehr Vorstellung sind, sondern zu einer Realität generiert sind.

Ob es eine solche Dystopie tatsächlich geben wird, ist fraglich, aber darüber lassen sich Fragen formulieren, die in erster Linie auf den Funktionswandel von Technologien hinweisen, der sich häufig nicht eindeutig vorhersagen lässt:

- Was sind die Ziele einer technischen Anwendung?
- Welche Diskurse werden bemüht um eine Technologie einzuführen?
- Ist sie dafür passend oder geht es nur um die Technologie selbst?
- Inwiefern profitiert die Gesellschaft als Ganzes davon und nicht nur kleine Gruppen?
- Wenn nur kleine Gruppen, wie lässt sich das begründen? Und um welche Art von Gruppen geht es dann im Speziellen?
- Ließe sich eine Anwendung ausweiten auf andere Bereiche?
- Wie werden Technologien begründet, ist Sicherheit der tatsächliche Antrieb oder gibt es andere Begründungen?
- Welche Vorstellungen, Hoffnungen oder Bedeutungen sind mit Technologien oder den betroffenen Kontexten und Anwendungsfeldern verbunden?

Generell gilt es zu fragen, wie in den fraglichen Bereichen Technologie bisher angewendet wurde, wie Menschen generell Technologie verstehen, und wie ganz praktisch das Verständnis von Technologie im persönlichen, privaten und öffentlichen Leben ist. Letztlich bedeutet das im Zusammenhang mit Sicherheit die Verbindungen von Sicherheit, Technologien, Bedeutungen von Technologien und politischen Wünschen zu untersuchen, damit es nicht zu unerwünschten Nebeneffekten kommt, die möglicherweise Freiheiten einschränken oder Rechte verletzen können. Und es muss vermehrt über Sicherheit im Kontext nachgedacht werden, was auch bedeutet über die relative Bedeutung von Sicherheit zu reflektieren. So kann angesichts von 1,6 verletzten Personen pro Spieltag in der 1. und 2. Bundesliga (für die Saison 2011/212 nach ZIS[17]) nicht von einer möglichen Unsicherheit in deutschen Stadien gesprochen werden, obwohl eine öffentliche Debatte deutlich Schlimmeres vermuten lässt. Und dennoch (oder gerade wegen der öffentlichen Debatte) wird weiterhin an neuen Sicherheitsmaßnahmen in und vor Stadien, rund um das Gesellschaftsereignis Fußball oder anderen Mega-Events gearbeitet. Die Begriffe der (Un-)Sicherheit werden inflationär benutzt, was zu einer Verschiebung von Wahrnehmung führt, den Sport aber zu einem Problem

[17] Zentrale Informationsstelle Sporteinsätze (ZIS): https://www.polizei-nrw.de/artikel__68.html (für alle Berichte). Aktuell: https://www.polizei-nrw.de/media/Dokumente/Behoerden/LZPD/ZIS_Jahresbericht_2013_14.pdf – die Zahlen haben sich nur unwesentlich verändert.

und damit zu einem fruchtbaren Einsatzfeld neuer Technologien werden lässt. Nicht von ungefähr gelten die Olympischen Spiele vor allem als Testfelder von Kontroll- und Überwachungstechnologien, die dann in anderer Form ihren Weg in die Städte finden (Haggerty & Bennett 2012; Sugden 2012).

5.3 Zusammenfassung: Technik und Überwachung

Die Implikationen technischer Innovationen auf Gesellschaft, politische und soziale Entwicklungen lassen sich nicht so ohne Weiteres vorhersagen. **Szenarien**, die wie in der Sicherheitsforschung üblich, vor allem ein Problem, eine Katastrophe oder eine Gefahr als Leitbild vorgeben, schaffen u.U. **Wirklichkeiten**, mit denen Technologien begründet werden können – unabhängig von ihrem tatsächlichen Eintreffen oder Vorhandensein. Solchermaßen gestaltete Szenarien sind für die Beantwortung gesellschaftlicher Zukunftsfragen unbrauchbar.

Konsequenzen und Implikationen lassen sich nicht von der Beschaffenheit der Technologien selbst ableiten (zumindest nicht unbedingt und allein), sondern derartige Analysen müssen den Kontext möglicher Anwendungen miteinbeziehen, ebenso wie die **Bedeutung von Technologie als Symbol** für oder gegen etwas. **Konsequenzen** können sowohl Individuen betreffen, als auch die Gesellschaft als Ganzes; Beobachtete ebenso wie die Bediener von Technologien; Politik, im Sinne Diskurs-gesteuerter Begründungszusammenhänge ebenso, wie den **Widerstand gegen eine Technologie**. Implikationen sind vielfältig und berühren **nicht allein den Datenschutz**, sondern möglicherweise andere **Freiheiten** oder **Rechte**, **Gewohnheiten** oder **gesellschaftliche Strukturen**, so dass technische Lösungen sozialer oder politischer Probleme nicht vom Reißbrett aus geplant und durchgeführt werden können. Und es darf dabei nicht in den Hintergrund geraten, dass die BürgerInnen Referenzobjekt der Sicherheit sind. Es geht darum gerade die Risiken zu minimieren, von denen diese selbst betroffen sein könnten. **BürgerInnen dürfen im Sinne der Sicherheitsmaßnahmen nicht selbst das Risiko werden** und somit zum Objekt der Sicherheit, vor dem es zu schützen gilt.

Technologien als Teil von **Sicherheitsfantasien** blenden andere Realitäten aus und verbauen eine eingehende Analyse von Wirkung, Ursache sowie den Interdependenzen von Technologie, Alltagspraktiken und Gesellschaft. So verhindern Sicherheits-fantasien den Blick auf ein Miteinander, wenn Sicherheit vor allem Schutz vor einem wie auch immer ausgestalteten Feind von außen (oder innen) ist. Die Abwehr von Feinden ist aber anders zu bewerten als der Umgang mit Problemen, die eigentlich keine Sicherheitsprobleme sind. Das bedeutet auch, dass in diesem Zusammenhang Risiken und Kosten ihrer Eindämmung besser berechnet werden müssen, bevor sie sich selbst unglaubwürdig machen. Die ungenügenden Kontrollen an Flughäfen sind ein Beispiel, ein weiteres liefert James Rinsen (2014), der vorrechnet, dass sich die Kosten des US-

amerikanischen Krieges gegen den Terror (im In- und Ausland) erst dann wirklich rechnet, wenn jährlich 1667 Terroranschläge in den USA stattfinden würden. Auch wenn es gerade in der Natur von Risiken liegt, dass man möglicherweise mehr Mittel aufwendet, als das Nicht-Eintreffen eines Ernstfalles kostet, so zeigt Rinsen vor allem, wie sich die Sicherheits- und Überwachungsindustrie anhand der Sicherheitsfantasien selbst aufbläht. **Sicherheit ist auch immer ein Geschäft. Risiken sind dabei das zentrale Verkaufsargument.**

6. Handlungsempfehlungen für die Sicherheitsforschung im Kontext von Überwachung

Empfehlungen hängen immer ein wenig davon ab wem was empfohlen wird. Im Falle der Sicherheitsforschung gibt es verschiedene Akteursgruppen, denen man unterschiedliches raten möchte – Politik, Wissenschaft sowie eine eher unbestimmte Gruppe ziviler/staatlicher Akteure und Unternehmen. In letzterer sind Überschneidungen nicht selten, was nicht heißt, dass es keine zu den anderen Gruppen gibt: Wissenschaftler, die beratend für Unternehmen tätig sind, staatlich-zivile Akteure, die in der Politik eine Rolle spielen. Im Bereich der Politik könnte man begründet unterscheiden zwischen Politikern (Abgeordneten, Ministern, öffentlicher Verwaltung) und solchen Akteuren, die eher praktisch mit Sicherheit zu tun haben wie Polizei, Feuerwehr, Militär usw. Diese sind hier jedoch der dritten Gruppe zugeordnet worden, da sie eher Profiteure der Sicherheitsforschung sind, weniger ihr Auftraggeber, und darüber hinaus zur Politik in einem Spannungsfeld stehen können, z.B. im Falle von den Konzepten innerer Sicherheit durch die Politik und den Wünschen und Anforderungen der Polizei selbst, die letztlich aber nicht selbst entscheiden kann. Es wird hier davon ausgegangen, dass die gemachte Unterteilung, die Gruppen entsprechend einer mehr oder weniger hinreichend unterschiedlichen jeweils eigenen Logik unterscheidet:

- **Politik**: Ausübung von Macht, Gestaltung der Politik und grundlegend verantwortlich für die zivile und militärische Sicherheit (die Überschneidungen werden auch in beiden Handlungsempfehlungen eine Rolle spielen)

- **Wissenschaft**: Erkenntnisinteresse, Generierung von Wissen, Berater der Politik, Finanzierung der eigenen Forschung

- **Unternehmen / zivile und staatliche Akteure:** Profit (monetär und symbolisch), praktischer Nutzen von Innovationen

Es wird deutlich, dass Aspekte wie Macht und Profit durchaus austauschbar sind, diese aber nicht zu den grundlegend definierenden Faktoren aller Gruppen gehören. Dennoch werden diese (und andere) Aspekte in den folgenden Handlungsempfehlungen bei allen Gruppen eine Rolle spielen. Damit die folgenden Empfehlungen nicht nur lose Ratschläge sind, sollen sie drei übergeordneten Prinzipien folgen: **Kommunikation**, **Reflexion** und **Transparenz.**

Mit **Kommunikation** ist sowohl eine **öffentliche Kommunikation** im Sinne eines Dialoges mit der Öffentlichkeit gemeint, als auch eine Kommunikation über Ziele, Strategien und Vorstellungen bezüglich verwendeter Konzepte von Sicherheit **zwischen den Partnern** beliebiger Sicherheitsforschungsprojekte.

Reflexion meint das Nachdenken über das eigene Handeln. Die Beweggründe einer Forschung, einer Politik sowie deren möglichen Konsequenzen, jenseits erhoffter Effekte, sollen in der Forschung von jedem Partner und jedem beteiligten Akteur sowohl einzeln/individuell, als auch gemeinsam reflektiert werden. Der Kern dieses Grundprinzips ist Verantwortung für das eigene Handeln zu übernehmen, insbesondere im Hinblick auf die Installation technischer Innovationen im Rahmen einer Lösung gesellschaftlicher Probleme.

Daran schließt das dritte Grundprinzip unmittelbar an: **Transparenz**. Verantwortung kann nur übernommen werden – und im Gegenzug als Merkmal für Güte beansprucht werden – wenn Klarheit über das eigene Tun und die dahinter stehenden Motivationen und Verbindungen nach außen herrscht.

Auf dieser Grundlage sind die folgenden Handlungsempfehlungen entsprechend der drei Gruppen unterteilt. Dass sich dabei Unterscheidungen ergeben, ist selbstverständlich. Dennoch denke ich, dass eine Trennung die Empfehlungen übersichtlicher und letztlich auch trennschärfer und damit u.U. auch verbindlicher machen.

6.1 Politik

- Sicherheit ist als gesellschaftliche Aufgabe zu begreifen, nicht allein als eine politische. Das bedeutet die möglichst breite Einbeziehung unterschiedlicher Akteure auf allen Ebenen, z.B. durch partizipative Verfahren, Zukunftswerkstätten, o.ä..

- Etablieren einer Kultur des Risikos und der Unsicherheit, wie z.B. von Bonß gefordert wird (vgl. Bonß 2011). Auch wenn dieses einen langen und schwierigen Prozess bedeutet, so müssen Maßnahmen unternommen werden, die damit einen Anfang machen. Das bedeutet vor allem eine Reflexion über den verwendeten Sicherheitsbegriff, insbesondere einen politisch-strategischen Sicherheitsbegriff, der bislang zu eng auf das zugeschnitten ist, was man mit innerer oder äußerer Sicherheit verbindet. Wichtig anzumerken ist, dass Unsicherheit oder Risiken hier nicht im Sinne einer neoliberalen Ideologie zu verstehen sind, die das Individuum auf eine falsch verstandene eigene Verantwortung zurückwirft, mit dem Ziel den Staat aus Kernaufgaben der gesellschaftlichen und sozialen Sicherung zurückzuziehen. Vielmehr ist hiermit die Aufforderung zu einer reflexiven Politik im Bereich Sicherheit gemeint, die sowohl über den Begriff der Sicherheit diskutiert, seine vielfältigen Dimensionen, aber vor allem die Grenzen von Sicherheit thematisiert.

- Es muss eine Kommunikation über die Zusammenhänge von Technologie und Sicherheit auf der einen und den als problematisch oder risikohaft identifizierten Bereichen von Gesellschaft auf der anderen Seite stattfinden. Sicherheit kann nicht ausschließlich als technisch zu lösendes Problem angesehen, sondern muss in seinen

durchaus vielfältigen Dimensionen analysiert werden. Eine Zuspitzung auf Technologie, sowie ein Konzentration auf die Abwehr von Gefahren sowie der Identifikation von Risiken bringt es auch mit sich die BürgerInnen selbst als solche zu begreifen. Eine bessere Kommunikation über Risiken und eine Transparenz der Einschätzung kann hier u.U. mehr Verständnis generieren. Die ideale Form der Kommunikation hierbei wäre ein Dialog mit Wissenschaft und anderen Akteuren.

- Vorsicht vor Symbolpolitik. Der Einsatz von Technik zur schnellen Reparatur aufkommender Probleme, deren Wirkung bestenfalls symbolhaft bleibt, ist zu unterbinden. Bodycams sind ein Beispiel einer solchen Reaktion, Videokameras in der Öffentlichkeit in der Regel auch. Der Einsatz von Technologie als Ausdruck eigener Handlungsstärke ist überflüssig und zumeist kontraproduktiv, weil man neue Probleme schafft, neue Begehrlichkeiten nach einer vermeintlichen Lösung weckt, die nur deshalb mehr von demselben fordert, weil es gut aussieht, aber nicht, weil es unbedingt hilft oder dem adressierten Problem angemessen ist.

- Technologie als Instrument der zivilen Sicherheit bedarf immer der Evaluation Um der Crux zu entgehen einer Technologie den Gewinn von Sicherheit zuzuschreiben, aber das ethische Dilemma ihrer Abschaffung nicht tragen zu wollen, muss bereits vor der Einführung über die unabhängige Evaluation einer Maßnahme nachgedacht werden. Diese muss, unter der Maßgabe der Beendigung oder Veränderung von Technologie und ihres Einsatzes, verbindlich sein.

- Suche nach vorhandenen oder zu schaffenden Alternativen, die nicht primär auf einer Technologie basieren. Dabei sind weitere (zivil-)gesellschaftliche Akteure einzubinden, um letztlich auch der abwehrenden Logik von Sicherheit zu entgehen. Das bedeutet auch politische Utopien oder wenigstens eine politische Kreativität zu entwickeln, die in reflexiver Weise und auf entsprechender Forschung basierend nach neuen Modellen sucht und diese politisch skizziert und umsetzt – Friedenskonzepte statt Sicherheitspolitik, Konfliktlösungen anstatt technischer Innovationen, technische Innovationen nicht zur Abwehr der Anderen (des Risikos), sondern zum Vorteil und Nutzen dieser Anderen (z.B. Flüchtlingspolitik als Entwicklungspolitik begreifen, nicht als Ansporn für bessere, technologisiertere Grenzen).

- Die Transparenz personeller und institutioneller Verquickungen ist elementar um Vertrauen zu schaffen und Verantwortung deutlich zu machen. Sicherheitsforschung darf nicht zu einem geschönten Begriff für Industriepolitik werden, in der Aufträge vergeben werden, deren Produkte dann wiederum als Ausdruck neuer Gefahren gelesen werden – sozusagen von der Lösung auf das (nicht vorhandene) Problem schließen, und so die Spirale aus Gefahr, Risiko, Sicherheit und technischer Lösung weiter befeuern. Politik selbst muss sich der Frage stellen wie sie mit der Industrie zusammenhängt? Weiterhin die Gründe von politischen Forderungen erörtern? Zum

Beispiel wäre es angebracht für die Politik zu diskutieren, ob ein tatsächliches Risiko oder eine drohende Unsicherheit die tatsächliche Motivation für eine Forderung sind oder viel eher eine auf Profit zielende personelle Verbindung?

6.2 Wissenschaft

- Wissenschaft muss ihre Bedeutung in Bezug auf Sicherheitsforschung jenseits von Machbarkeit (z.B. in den Ingenieurwissenschaften) oder einer reinen Akzeptanzforschung (als welche die Sozialwissenschaften oft missverstanden werden) deutlicher herausstellen. Das bedeutet auch, dass Wissenschaft aktiv auf die Gestaltung einer anderen Sicherheitsforschung einwirken muss.

- Wissenschaft muss in jedem Fall Verantwortung für ihre Konzepte oder Produkte übernehmen. Die Entwicklung von Überwachungstechnologie kann nicht auf Inselpositionen beschränkt bleiben etwas zwar entwickelt zu haben, aber für die Konsequenzen der Anwendung andere verantwortlich machen. Vielmehr muss der Austausch und die kritische Reflexion über mögliche Konsequenzen bereits im Entwicklungsprozess angelegt werden. Das bedeutet mehr als nur nach rechts- oder sozialverträglichen Bauelementen oder Versionen einer Technologie zu suchen, sondern im Rahmen von Sicherheit auch über Sinn und weiteren Zweck zu reflektieren.

- Um dieser Verantwortung nachzukommen, bedarf es im Forschungsprozess einer verbesserten Kommunikation, sowie einer Zusammenarbeit und des echten Austausches beteiligter Disziplinen soweit möglich auch in der Forschung angelegt. Interdisziplinarität darf nicht nur im Titel stehen und als autonomes Nebeneinander verstanden werden.

- Und schließlich gilt auch für die Wissenschaft eine Forderung der Transparenz möglicher personeller Verquickungen mit Industrie, Forschungsförderern oder der Politik. Angesichts knapper werdender Grundfinanzierungen von Wissenschaft an den Universitäten, ist gerade die Finanzierung von Forschung jeder Disziplin immer auch Interessengeleitet und bedarf somit einer Transparenz der eigenen Motivation und möglicher Verflechtungen – insbesondere wenn daraus Forderungen nach mehr Sicherheit oder der Feststellung mutmaßlicher Sicherheitsprobleme erwachsen.

- Es bedarf des offenen Diskurses und der Diskussion auch mit Akteuren außerhalb der Wissenschaft.

- Wissenschaft muss sich einbringen und Möglichkeiten für einen Dialog schaffen. Wobei zugegebenermaßen die Wissenschaft am ehesten für diesen Dialog bereitsteht,

da sie im Gegensatz zu Politik und Unternehmen der schwächste der Akteure dieser Konstellation ist und in vielerlei Hinsicht von den anderen abhängt.

- Wissenschaft muss sich politisch positionieren, nicht strategisch, sondern grundsätzlich, um der Gefahr zu entgehen, als beliebig wahrgenommen zu werden. Das bedeutet eine Reflexion der eigenen Arbeit und eine Kommunikation nach außen, besonders in kritischen Zusammenhängen, z.B. Forschung und Entwicklung in so genannten dual-use-Zusammenhängen.

- Es bedarf eines klar kommunizierten Begriffes von Sicherheit. Dieser muss und kann nicht einheitlich sein, aber die jeweilige Sichtweise sollte ausgearbeitet genug sein, dass sie nicht einfach ein beliebig zu füllendes Korsett darstellt. Wer zu Sicherheit forscht – gleich ob im Zusammenhang mit technischen Innovationen für die Sicherheit oder im Rahmen eines kritisch orientierten Ansatzes (z.B. in den Sozialwissenschaften) – braucht einen definierten Begriff.

6.3 Unternehmen / zivile und staatliche Akteure

- Transparenz der Interessen und Motivationen. Während bei Unternehmen die Motivation in der Regel offensichtlich ist – Profit und Unterstützung bei der Entwicklung technischer Innovationen – ist sie das bei zivilen und staatlichen Akteuren nicht immer. Bei der Polizei oder der Feuerwehr muss es nicht zwingend um ein identifiziertes Sicherheitsproblem gehen, welches vordergründig geltend gemacht wird. Auch hier ist bei knappen Kassen öffentlicher Haushalte davon auszugehen, dass Sicherheitsprobleme vorgeschoben werden können, um die eigene Bedeutung herauszustellen, z.B. über Stellen oder weitere Haushaltsmittel. Das gilt auch für zivilgesellschaftliche Akteure z.B. in der Drogenbekämpfung oder anderen Zusammenhängen/Feldern, wobei es sich hier nicht unbedingt um technische Innovationen handelt. Ähnliches gilt für die Transparenz bei personellen und institutionellen Verbindungen mit den Bereichen Politik in der Rolle des Geldgebers mit der Hoheit über den Bedarf, sowie der Wissenschaft als Legitimationsinstanz oder Dienstleister im Bereich Forschung.

- Kommunikation mit den anderen Akteursgruppen über konkrete Maßnahmen hinweg. Das bedeutet auch die Reflexion über den Begriff der Sicherheit. Sicherheit darf nicht ausschließlich normativ und weitgehend undefiniert verwendet werden. Auch wenn für manche Akteure ein leerer Begriff von Vorteil sein mag, weil er in der Praxis dann keine Einschränkungen verlangt, so ist im Sinne einer Offenheit, einer transparenten Politik und eines reflexiven Umganges eine bessere und trennschärfere Beschäftigung mit dem Phänomen dringend notwendig.

- Sicherheit darf deshalb nicht als catch-all-Begriff verwendet werden. Vielmehr sollten die Probleme, um die es im Zusammenhang mit den beteiligten Akteuren tatsächlich geht, benannt werden. So geht es im Zusammenhang mit öffentlicher Videoüberwachung nicht immer um Sicherheit, sondern auch um symbolische Politik, um das Setzen von Zeichen, nicht um Kriminalität, sondern um ein besseres Stadtbild usw. Das sollte dann auch ehrlicherweise so kommuniziert werden.

Wie immer Akteure aus den drei Bereichen im Zusammenhang mit Sicherheit im Kontext von Überwachung verwoben sind, sie müssen den Prämissen Kommunikation, Reflexion und Transparenz folgen. Nur auf diese Weise kann sich aus dem bisher recht starren Konzept von Sicherheit, wie es bisher im Zusammenhang mit Überwachung und der Sicherheitsforschung verwendet wird, ein besser handhabbares Konzept entwickeln. Letztlich muss es das Ziel einer freiheitlichen Gesellschaft sein, die Überwachung der Bürger, insbesondere jede verdachtslose und flächendeckende Überwachung und Kontrolle, auf ein Minimum zu beschränken und für Konflikte andere Lösungen, als immer neue technische Innovationen entsprechend eines undefinierten Sicherheitsbegriffes, zu finden. Sicherheit darf sich nicht auf die Abwehr (und Überwachung und Kontrolle) eines mutmaßlichen gefährlichen Anderen beschränken, potenzielle Risiken dürfen nicht zur Argumentationsgrundlage für ausufernde Überwachung werden. Die Sicherheit der BürgerInnen, darf nicht zur Sicherheit vor den BürgerInnen mutieren.

Letztlich bedeutet dies, dass für eine Zusammenarbeit in der Sicherheitsforschung Standards geschaffen werden müssen, die sich auf die drei Prämissen beziehen und somit als flexibler Hintergrund für jede Kooperation ein Mindestmaß an Verhalten entsprechend der gemachten Empfehlungen einfordern. Verantwortung, Vertrauen und eine freiheitliche Gesellschaft, in der der Bürger im Mittelpunkt steht, würden davon enorm profitieren.

7. Literatur

Ackermann, Ulrike; Baumann, Max-Otto; Berlinghoff, Marcel (Hg.) (2013): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter. Frankfurt am Main, Humanities Online.

Adamowsky, Natascha (2010): Das Wunder in der Moderne. Eine andere Kulturgeschichte des Fliegens. München, Fink.

Adey, Peter (2004): Secured and sorted mobilities: examples from the airport. Surveillance and Society, 1(4), S. 500–519.

Adey, Peter (2010): Aerial Life. Spaces. Mobilities. Affects. Chichester (2010).

Albrechtslund, Anders; Louise Nørgaard Glud (2010):Empowering Residents: A Theoretical Framework for Negotiating Surveillance Technologies, Surveillance & Society, 8 (2010), S. 235–50.

Algazi, Gadi (2008): Sperrzonen und Grenzfälle. Beobachtungen zu Herrschaft und Gewalt im kolonialen Kontext zwischen Israel und Palästina. In: Alf Lüdtke & Michael Wildt (Hg.): Staats-Gewalt: Ausnahmezustand und Sicherheitsregime. Historische Perspektiven. Göttingen, Wallstein. Amin & Thrift 2002.

Ammicht Quinn, Regina (Hg.) (2014): Sicherheitsethik. Wiesbaden: Springer Fachmedien Wiesbaden GmbH (Studien zur Inneren Sicherheit, 16).

Ammicht Quinn, Regina; Nagenbor,Michael; Rampp, Benjamin; Wolkenstein, Andreas (2014): Ethik und Sicherheitstechnik. Eine Handreichung. In: Regina Ammicht Quinn (Hg.): Sicherheitsethik. Wiesbaden: Springer Fachmedien Wiesbaden GmbH (Studien zur Inneren Sicherheit, 16), S. 277–296.

Ammicht Quinn, Regina; Nagenborg, Michael; Rampp, Benjamin; Traut, Andreas (2010): Körperscanner. Sicherheiten und Unsicherheiten. In: Forum Kriminal-prävention (1), S. 14–20.

Ammicht Quinn, Regina; Rampp, Benjamin (2009): The Ethical Dimension of Terahertz and Millimeter-Wave Imaging Technologies. Security, Privacy, and Acceptability. In: Halvorson, Craig S. (Hg.): SPIE Proceedings. Defense, Security and Sensing, May 05, 2009. Optics and Photonics in Global Homeland Security V and Biometric Technology for Human Identification VI. Orlando.

Amoore, Louise (2013): The Politics of Possibility. Risk and Security Beyond Probability. Durham: Duke University Press.

Andelfinger, Volker P.; Hänisch, Till (Hg.) (2015): Internet der Dinge. Technik, Trends und Geschäftsmodelle. Wiesbaden: Springer Gabler.

Anderson, Chris (2013): Makers. Das Internet der Dinge: die nächste industrielle Revolution. 1. Aufl. München, Carl Hanser Fachbuchverlag.

Andrejevic, Mark (2005): The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. In: Surveillance & Society 2(4), S. 479-497.

Andrejevic, Mark; Gates, Kelly (2014): Big Data Surveillance. Introduction. In: S&S 12 (2), S. 185–196. Online verfügbar unter http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/5242.

Anonymous (2014): Deep Web. Die dunkle Seite des Internets. 1. Aufl. Berlin, Blumenbar.

Armstrong, Gary; Norris, Clive (2010): The Maximum Surveillance Society. The Rise of CCTV. Oxford, Berg.

Aumann, Philipp (2013): Control. Kommunikationstechniken als Motoren von Entprivatisierung und Fremdsteuerung. In: Ulrike Ackermann, Max-Otto Baumann und Marcel Berlinghoff (Hg.): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter. Frankfurt am Main, Humanities Online, S. 131–150.

Axelsson, Per; Sköld, Peter (Hg.) (2011): Indigenous Peoples and Demography. The Complex Relation between Identity and Statistics. First paperback edition: Berghahn Books.

Bachmannn, Barbara (2014): Dein Haus kennt Dich, in Die Zeit, Nr. 50, 4. Dezember 2014, S. 12.

Baker, Judy L.; Dickson, Eric; Hoornweg, Daniel; Tiwari, Asmita (2012): Urban Risk Assessments. Understanding Disaster and Climate Risk in Cities. Washington, DC, World Bank.

Ball, Kirstie; Snider, Laureen (Hg.) (2013): The Surveillance-Industrial Complex. A Political Economy of Surveillance. London, Routledge.

Bartl, Gabriel; Gerhold, Lars; Wählisch, Mathias (2014): Towards a theoretical framework of acceptance for surveillance systems at airports, in Proceedings of the 11th International ISCRAM Conference – University Park, Pennsylvania, USA, May 2014 S.R. Hiltz, M.S. Pfaff, L. Plotnick, and P.C. Shih (eds).

Baudrillard, Jean (1994): Simulacra and Simulation. Michigan.

Bauman, Zygmunt (2009): Leben als Konsum. Hamburg, HIS.

Bauman, Zygmunt (2003): Flüchtige Moderne. 6. Aufl. Frankfurt am Main, Suhrkamp.

Bauman, Zygmunt; Lyon, David; Jakubzik, Frank (2013): Daten, Drohnen, Disziplin. Ein Gespräch über flüchtige Überwachung. 2. Aufl. Berlin: Suhrkamp.

Bächle, Thomas Christian; Thimm, Caja (Hg.) (2014): Mobile Medien – mobiles Leben. Neue Technologien, Mobilität und die mediatisierte Gesellschaft. Berlin, LIT (Bonner Beiträge zur Onlineforschung, 3).

Beck, Ulrich (1986): Die Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt a. Main, Suhrkamp.

Beck, Ulrich (2008): Weltrisikogesellschaft. Auf der Suche nach der Verlorenen Sicherheit. München, Oldenbourg Wissenschaftsverl (31).

Beck, Ulrich; Mulsow, Martin (Hg.) (2014): Vergangenheit und Zukunft der Moderne. 1. Aufl. Berlin: Suhrkamp (Edition Suhrkamp, 2685).

Beckedahl, Markus; Lüke, Falk (2012): Die digitale Gesellschaft. Netzpolitik, Bürgerrechte und die Machtfrage. 1. Aufl. dtv.

Becker, Matthias (2010): Datenschatten. Auf dem Weg in die Überwachungs-gesellschaft? 1. Aufl. Hannover, Heise (Telepolis).

Belina, Bernd (2007): Zur Kritik von Kriminalgeographie und Kriminalitätskartierung und warum deren heutige Bemühungen noch hinter Quetelet zurückfallen. In: Tzschaschel, Sabine; Wild, Holger; Lentz, Sebastian (Hg.): Visualisierung des Raumes. Karten machen – die Macht der Karten (= Forum IfL 6). Leipzig, IfL, S. 241-255.

Belina, Bernd (2011): Raum, Überwachung, Kontrolle. Vom staatlichen Zugriff auf städtische Bevölkerung Münster, Westf. Dampfboot.

Belina, Bernd (Hg.) (2011): Urbane Differenzen. Disparitäten innerhalb und zwischen Städten. 1. Aufl. Münster, Verl. Westf. Dampfboot (Raumproduktionen: Theorie und gesellschaftliche Praxis).

Bellanova, Rocco; Fuster, Gloria González (2013): Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices, International Political Sociology, 7 (2013), S. 188–209.

Bennett, Colin J. (2011): In Defense of Privacy: The Concept and the Regime', Surveillance & Society, 8 (2011), 485–96.

Bennett, Colin J.; Haggerty, Kevin D.; Lyon, David; Steeves, Valerie (Hg. 2014): Transparent Lives: Surveillance in Canada, Athabasca University Press.

Bennett, Colin J. (2008): The Privacy Advocates Resisting the Spread of Surveillance. Cambridge, MIT Press.

Bennett, Colin J.; Haggerty, Kevin D. (Hg.) (2012): Security Games. Surveillance and Control at Mega-Events, Taylor & Francis.

Bennett, Trevor; Holloway, Katy; Farrington, David P. (2006): Does Neighborhood Watch Reduce Crime? A Systematic Review and Meta-Analysis. In: Journal of Experimental Criminology 2 (4), S. 437–458. DOI: 10.1007/s11292-006-9018-5.

Bennett, Colin J.; Lyon, David (Hrsg. 2008): Playing the Identity Card. London/New York, Routledge.

Berchthold, Nicola (2007): Spuren des "Berufsverbrechers". Die Daktyloskopie als Identifizierungstechnik in deutschen Großstädten um 1900. In: Nils Zurawski (Hg.): Sicherheitsdiskurse. Angst, Kontrolle und Sicherheit in einer "gefährlichen" Welt. Frankfurt am Main, Lang, S. 39–60.

Berger, Peter; Keller, P. A.; Klärner, A.; Neef, R.(Hg.) (2014): Urbane Ungleichheiten. Neue Entwicklungen zwischen Zentrum und Peripherie. Wiesbaden, Springer VS.

Bessis, Nik; Dobre, Ciprian (Hg.) (2014): Big Data and Internet of Things. A Roadmap for Smart Environments. Cham, Springer International Publishing (Studies in Computational Intelligence, 546). Online verfügbar unter http://dx.doi.org/10.1007/978-3-319-05029-4.

Bigo, Didier; Carrera, Sergio; Guild, Elspeth; Walker, R.B.J. (Hg.) (2010): Europe's 21st Century Challenge. Delivering Liberty. Farnham, Ashgate.

Bijker, Wiebe; Hughes, Thomas; Pinch, Trevor (Hg.) (2012): The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology. Anniversary ed. Cambridge, Mass, MIT Press.

Boersma, Kees; Wagenaar, F. P. (2012): Zooming in on ‘Heterotopia’. CCTV-operator Practices at Schiphol Airport. In: Information Polity 17 (1), S. 7–20.

Bogard, William (1996): The Simulation of Surveillance. Hypercontrol in Telematic Societies. Cambridge, Cambridge Univ. Press.

Bogard, William (2006): Welcome to the Society of Control. The Simulation of Surveillance Revisited. In: Haggerty, Kevin; Ericson, Richard (Hg.): The New Politics of Surveillance and Visibility. Toronto, Toronto Univ. Press.

Boghosian, Heidi (2013): Spying on Democracy. Government Surveillance, Corporate Power, and Public Resistance. San Francisco, City Lights Books.

Bogner, Alexander (2012): Gesellschaftsdiagnosen. Ein Überblick. Weinheim, Basel, Beltz Juventa.

Bogner, Alexander (2013): Ethisierung oder Moralisierung? Technikkontroversen als Wertkonflikte. In: Bogner, Alexander (Hg.): Ethisierung der Technik – Technisierung der Ethik. Der Ethik-Boom im Lichte der Wissenschafts- und Technikforschung. Baden-Baden, Nomos, S. 51–68.

Bogner, Alexander (Hg.) (2013): Ethisierung der Technik – Technisierung der Ethik. Der Ethik-Boom im Lichte der Wissenschafts- und Technikforschung. Baden-Baden: Nomos.

Bonß, Wolfgang (2011): (Un-)Sicherheit in der Moderne. In: Peter Zoche, Stefan Kaufmann und Rita Haverkamp (Hg.): Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. Bielefeld: Transcript-Verl (Sozialtheorie), S. 43–70.

Bourdin, Alain; Eckardt, Frank; Wood, Andrew (2014): Die ortlose Stadt. Über die Virtualisierung des Urbanen. Bielefeld, Transcript.

Bowker, Geoffrey C. & Star, Susan Leigh (1999): Sorting Things out. Classifications and its Consequences. Cambridge, MIT Press.

Bökenkamp, Gérard (2012): Das Internet zwischen Datenschutz und Informationsfreiheit. Liberales Institut der Friedrich-Naumann-Stiftung für die Freiheit (Hg.)(PositionLiberal, 2011, S. 100).

Browne, S. (2010): Digital Epidermalization. Race, Identity and Biometrics. In: Critical Sociology 36 (1), S. 131–150. DOI: 10.1177/0896920509347144.

Budd, Lucy; Warren, Adam; Bell, Morag (2015): Aviation biosecurity: protecting people, places and planes from biological threats. In Herlyn, Gerrit; Zurawski, Nils (Hg.)(2015a): Achtung Sicherheitskontrollen! – Flughäfen, Kultur, Un/Sicherheiten. Münster, Lit.

Budd, Lucy; Bell, Morag; Brown, Tim (2009). „Of plagues, planes and politics: Controlling the global spread of infectious diseases by air“. Political Geography 28 (7). S. 426–35. doi:10.1016/j.polgeo.2009.10.006.

Bullock, Karen (2014): Citizens, Community and Crime Control. Basingstoke, Palgrave Macmillan.

Byrne, James M.; Pattavina, April (2013): Technological Innovation and Offender Reentry. In: Stephane Leman-Langlois (Hg.): Technocrime, Policing and Surveillance. London, Routledge (Routledge frontiers of criminal justice, 3), S. 110–132.

Callon, Michael (2012): Society in the Making. The Study of Technology as a Tool for Sociological Analysis. In: Bijker, Wiebke; Hughes, Thomas; Pinch, Trevor (Hg.): The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology. Anniversary ed. Cambridge, Mass, MIT Press, S. 77–98.

Caputo, Tony C. (2010): Digital Video Surveillance and Security. Amsterdam, Butterworth-Heinemann/Elsevier.

Cardullo, Paolo (2014): Sniffing the City. Issues of Surveillance in Inner City London. In: Visual Studies 29 (3), S. 285–293. DOI: 10.1080/1472586X.2014.941550.

Carr, Nicholas (2009): The Big Switch – Der große Wandel. Cloud Computing und die Vernetzung der Welt von Edison bis Google. 1. Aufl. Heidelberg, mitp.

Castells,Manuel (1996): The Information Age: Economy, Society and Culture, Vol I: The Rise of the Network Society. Oxford, Blackwell.

Chao, Chia-Chen; Yang, Jiann-Min; Jen, Wen-Yuan (2007): Determining Technology Trends and Forecasts of RFID by a Historical Review and Bibliometric Analysis from 1991 to 2005. In: Technovation 27 (5), S. 268–279. DOI: 10.1016/j.technovation.2006.09.003.

Clark, Peter (2009): European Cities and Towns 400-2000. Oxford, Oxford University Press.

Clark, David (2004): Urban World/Global City: Taylor & Francis.

Coleman, Roy (2005): Surveillance in the City. Primary Definition and Urban Spatial Order. in Crime Media Culture 1 (2), S. 131–148.

Coll, Sami (2013): Consumption as Biopower: Governing Bodies with Loyalty Cards. Journal of Consumer Culture 13 (3): S. 201–20. doi:10.1177/1469540513480159.

Coll, Sami (2012): The social dynamics of secrecy: Rethinking information and privacy through Georg Simmel. International Review of Information Ethics 17, S.15–20.

Coll, Sami (2014): Power, Knowledge, and the Subjects of Privacy: Understanding Privacy as the Ally of Surveillance. Information, Communication & Society 17 (10) S. 1250–63. doi:10.1080/1369118X.2014.918636.

Cukier, Kenneth; Mayer-Schönberger, Viktor (2013): Big Data. Die Revolution, die unser Leben verändern wird. 1. Aufl. München, Redline-Verl.

Czerwinski Stefan & Zurawski, Nils (2008): Knowledge and Meaning – Views on Safety, Crime and CCTV. Discussing Results from a Survey. In: Surveillance & Society 5 (1), S. 51-72.

Czerwinski, Stefan (2007): Kriminalisierung von Stadträumen durch Videoüberwachung. In: Juleka Schulte-Ostermann, Rebekka Henrich & Veronika Kesoglou (Hg.): Praxis, Forschung, Kooperation – Gegenwärtige Tendenzen in der Kriminologie. Frankfurt a. Main, Verlag für Polizeiwissenschaften.

D'Aprile, Dorothee (Hg.) (2014): "Moloch, Kiez und Boulevard". Die Welt der Städte (Edition Le Monde diplomatique, 14).

Daase, Christopher (2013): Verunsicherte Gesellschaft – überforderter Staat. Zum Wandel der Sicherheitskultur. Frankfurt am Main, Campus-Verl.

Daase, Christopher; Offermann, Philipp; Rauer, Valentin (Hg.) (2012): Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr. 1. Aufl. Frankfurt am Main, Campus Verlag (Sozialwissenschaften 2012).

Dashper, Katherine (Hg.) (2015): Sports Events, Society and Culture. London, Routledge.

De Lint, Willem (2002): The security double take: The political, simulation and the border. Surveillance & Society, 5(2).

Dickson, Eric; Baker, Judy L.; Hoornweg, Daniel; Tiwari, Asmita (2012): Urban Risk Assessments – Understanding Disaster and Climate Risk in Cities. Urban Development Series. Washington DC, World Bank.

Dolata, Ulrich (2013): The Transformative Capacity of New Technologies. A Theory of Sociotechnical Change. Hoboken: Taylor and Francis (Routledge Advances in Sociology).

Downing, Stephen (c2013): Technology and Crime Prevention. In: Kristine Levan und David A. Mackey (Hg.): Crime Prevention. Burlington, Mass: Jones & Bartlett Learning, S. 163–192.

Dünne, Jörg; Günzel, Stephan (Hg.): Raumtheorie. Grundlagentexte aus Philosophie und Kulturwissenschaft. Frankfurt a. Main, Suhrkamp.

Eckert, Svea (2014): Überwacht und ausgespäht. PRISM, NSA, Facebook & Co. Köln, Lingen.

Evers, Adalbert; Nowotny, Helga (1987): Über den Umgang mit Unsicherheit. Die Entdeckung der Gestaltbarkeit von Gesellschaft. Frankfurt/Main, Suhrkamp.

Filonenko, Alexander; Vavilin, Andrey; Kim, Taeho; Jo, Kang-Hyun: Augmented Reality Surveillance System for Road Traffic Monitoring, Bd. 8589, S. 310–317.

Foucault,Michel (1994): Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt am Main, Suhrkamp.

Friedman, Batya, Kahn Jr, P. H.; Hagman, J.; Severson, R. L.; Gill, B. (2006): The Watcher and the Watched: Social Judgments about Privacy in a Public Place, in Human-Computer Interaction, 21 (2006), S. 235–72.

Frois, Catarina (2013): Peripheral Vision. Politics, Technology, and Surveillance. Oxford, Berghahn.

Fussey, Pete; Klauser, Francisco (2014): Securitisation and the Mega-Event. An Editorial Introduction. In: The Geographical Journal, S. n/a. DOI: 10.1111/geoj.12101.

Garland, David (2008): Kultur der Kontrolle. Verbrechensbekämpfung und soziale Ordnung in der Gegenwart. Frankfurt/Main, Campus-Verl (Frankfurter Beiträge zur Soziologie und Sozialphilosophie).

Gaycken, Sandro; Kurz, Constanze (Hg.) (2008): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. transcript.

Geiselberger, Heinrich (Hg.) (2013): Big Data. Das neue Versprechen der Allwissenheit. 2. Aufl. Berlin: Suhrkamp (edition unseld Sonderdruck).

Gelernter, David (2013): The Danger to Privacy Posed by Technology and Culture Working Together. In: Ulrike Ackermann, Max-Otto Baumann und Marcel Berlinghoff (Hg.): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter. Frankfurt am Main, Humanities Online, S. 159–173.

Gerhold, Lars; Holtmannspötter, D.; Neuhaus, C.; Schüll, E.; Schulz-Montag, B.; Steinmüller, K.; Zweck, A. (2015): Standards und Gütekriterien der Zukunfts-forschung Ein Handbuch für Wissenschaft und Praxis. Wiesbaden, Springer.

Giddens, Anthony (1984): The Constitution of Society. Outline of the Theory of Structuration. University of California Press.

Gilliom, John; Monahan, Torin (2013): SuperVision. An Introduction to the Surveillance Society. Chicago, The Univ. of Chicago Press.

Giseke, Jens (2011): Die Stasi. 1945-1990. München, Pantheon.

Giulianotti, R.; Klauser, F. (2012): Sport Mega-Events and 'Terrorism'. A Critical Analysis. In: International Review for the Sociology of Sport 47 (3), S. 307–323. DOI: 10.1177/1012690211433454.

Giulianotti, Richard (2011): Sport Mega Events, Urban Football Carnivals and Securitised Commodification. The Case of the English Premier League. In: Urban Studies 48 (15), S. 3293–3310. DOI: 10.1177/0042098011422395.

Glasze, Georg / Pütz, Robert & Rolfes, Manfred (2005): Diskurs–Stadt–Kriminalität. Städtische Unsicherheiten aus der Perspektive von Stadtforschung und Kritischer Kriminologie. Bielefeld, transcript.

Gottschalk-Mazouz, Niels (2008): Risiko, Akzeptanz und Akzeptabilität. Was man von der Gentechnologie über Nanotechnologie lernen kann. In: Christoph Hubig und Peter Koslowski (Hg.): Maschinen, die unsere Brüder werden. Mensch-Maschine-Interaktion in hybriden Systemen. Paderborn, Fink (Ethische Ökonomie, 11), S. 173–189.

Graham, Mark; Zook, Matthew; Boulton, Andrew (2013): Augmented Reality in Urban Places. Contested Content and the Duplicity of Code. In: Transactions of the

Institute of British Geographers 38 (3), S. 464–479. DOI: 10.1111/j.1475-5661.2012.00539.x.

Graham, Stephen (2002): CCTV: The Stealthy Emergence of a Fifth Utility? Planning Theory & Practice 3 (2), S. 237-241.

Graham, Stephen (2005): Software-sorted Geographies. In: Progress in Human Geography 29 (5), S. 1-19.

Graham, Stephen (2010): Cities Under Siege. The New Military Urbanism. London, Verso.

Graham, Stephen; Wood, David (2003): Digitizing Surveillance. Categorization, Space, Inequality. In: Critical Social Policy 23 (2), S. 227–248. DOI: 10.1177/0261018303023002006.

Greenwald, Glenn (2014): Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München, Droemer.

Greenwald, Glenn (2014): No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State. 1. Aufl. New York, Metropolitan Books Henry Holt.

Grunwald, Armin (2008): Technik und Politikberatung. Philosophische Perspektiven. Frankfurt am Main, Suhrkamp (Suhrkamp-Taschenbuch Wissenschaft, 1901).

Grunwald, Armin (2010): Technikfolgenabschätzung. Eine Einführung. 2. Aufl. Berlin: Ed. Sigma (Gesellschaft, Technik, Umwelt, 1).

Guennoun, Mouhcine; Khattak, Saad; Kapralos, Bill; El-Khatib, Khalil: Augmented Reality-Based Audio/Visual Surveillance System. In: Conference: Haptic Audio visual Environments and Games, 2008. Haptic Audio visual Environments and Games, 2008, S. 70–74.

Gugerli, David (2009): Suchmaschinen. Die Welt als Datenbank. Frankfurt am Main, Suhrkamp.

Günzel, Stephan (Hg.) (2009): Raumwissenschaften. Frankfurt a. Main, Suhrkamp.

Haggerty, Kevin D. & Ericson, Richard V. (2000): The Surveillant Assemblage. In: British Journal of Sociology 51 (4), S. 605-622.

Haggerty, Kevin D. & Ericson, Richard V. (2006): The New Politics of Surveillance and Visibility. In: Kevin D. Haggerty & Richard Ericson (Hg.): The New Politics of Surveillance and Visibility. Toronto, Toronto Univ. Press.

Haggerty, Kevin D. (2006): The New Politics of Surveillance and Visibility. Toronto, Univ. of Toronto Press.

Halvorson, Craig S. (Hg.) (2009): SPIE Proceedings. Defense, Security and Sensing. Optics and Photonics in Global Homeland Security V and Biometric Technology for Human Identification VI. Orlando.

Hannah, Matthew (2010): Dark Territory in the Information Age. Learning from the West German Census Controversies of the 1980s. Farnham, Ashgate.

Harders, Immo (2014): Die elektronische Überwachung von Straffälligen. Entwicklung, Anwendungsbereiche und Erfahrungen in Deutschland und im europäischen Vergleich. Mönchengladbach, Forum-Verl. Godesberg (Schriften zum Strafvollzug, Jugendstrafrecht und zur Kriminologie, 46).

Harms, J. Menno (2011): Sicherheitsgewinn mit technologischen Innovationen (Schwerpunkt ITK). In: Peter Zoche, Stefan Kaufmann und Rita Haverkamp (Hg.): Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. Bielefeld, Transcript-Verl (Sozialtheorie), S. 29–34.

Häfele, Joachim (2013): Die Stadt, das Fremde und die Furcht vor Kriminalität. Wiesbaden, Springer VS.

Häußling, Roger (2014): Techniksoziologie. 1. Aufl. Stuttgart, UTB GmbH.

Hempel, Leon (2008): Die geschlossene Welt. Zur Politik der Überwachung am Beispiel von Videoüberwachung. In: Sandro Gaycken und Constanze Kurz (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Transcript, S. 79–101.

Hempel, Leon; Metelmann, Jörg (Hg.) (2005): Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. 1. Aufl. Frankfurt am Main: Suhrkamp (Suhrkamp-Taschenbuch Wissenschaft, 1738).

Hempel, Leon; Töpfer, Eric (2004): CCTV in Europe. Final Report. Urbaneye Working Paper No. 15. Berlin.

Hempel, Leon; Töpfer, Eric (2009): The Surveillance Consensus. Reviewing the Politics of CCTV in Three European Countries. In: European Journal of Criminology 6 (2), S. 157–177.

Hengartner, Thomas (2009): Von Schreib-, Sprech- und Denkmaschinen. Zum Verhältnis von Mensch, Kultur und Technik. In: Geisteswissenschaften in der Offensive: Hamburger Standortbestimmungen, S. 255–275.

Hengartner, Thomas (2012): Technik – Kultur – Alltag. Technikforschung als Alltagskulturforschung. In: Schweizerisches Archiv für Volkskunde 106, S. 117–139.

Hengartner, Thomas; Rolshoven, Johanna (Hg.) (1998): Technik – Kultur. Formen der Veralltäglichung von Technik – Technisches als Alltag. Zürich: Chronos.

Herlyn, Gerrit; Zurawski, Nils (2015a): Sicherheitsmaßnahmen am Flughafen und Identitätskonstruktionen: Kulturelle Identitäten als Bild, Praktik und Instrument. In: Fischer, Susanne & Masala, Carlo (Hg.): Innere Sicherheit nach 9/11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen? Wiesbaden 2015.

Herlyn, Gerrit; Zurawski, Nils (Hg.) (2015a): Achtung Sicherheitskontrollen! – Flughäfen, Kultur, Un/Sicherheiten. Münster, Lit.

Herlyn, Gerrit (2014): Passagierdifferenzierung als Social Sorting – Anmerkungen zur Diskussion um zukünftige Sicherheitsmaßnahmen am Flughafen aus kulturwissenschaftlicher Sicht, in Wagner, Katrin &, Wolfgang Bonß (2014): Risikobasiert versus One Size Fits All. Neue Konzepte der Passagierüberprüfung im Luftverkehr. Neubiberg, Universität der Bundeswehr München

Herlyn, Gerrit (2015): Randomly selected for additional Screening? Zur Kulturanalyse von Sicherheitsmaßnahmen am Flughafen, in Herlyn, Gerrit & Nils Zurawski (Hrsg. 2015a): Achtung Sicherheitskontrollen! – Flughäfen, Kultur, Un/Sicherheiten. Münster, Lit.

Hess, D. J.; Coley, J. S. (2014): Wireless Smart Meters and Public Acceptance. The Environment, Limited Choices, and Precautionary Politics. In: Public Understanding of Science 23 (6), S. 688–702. DOI: 10.1177/0963662512464936.

Heßler, Martina (2012): Kulturgeschichte der Technik. Frankfurt am Main, Campus.

Hilty, Lorenz M. (2012): Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern. Zürich, vdf Hochschulverlag (TA-SWISS, 57).

Hirschberger, Bernd (2015): Nacktscanner oder Körperscanner? – Freiheit vs. Sicherheit. In Herlyn, Gerrit; Zurawski, Nils (Hg.) (2015a): Achtung Sicherheitskontrollen! – Flughäfen, Kultur, Un/Sicherheiten. Münster, Lit.

Hirschfeld, Karin (2014): Telecare verändert die Pflege. Pro und Kontra des Einsatzes digitaler Überwachung. In: Mitbestimmung : das Magazin der Hans-Böckler-Stiftung / Hrsg.: Hans-Böckler-Stiftung, Mitbestimmungs- Forschungs- und Studienförderungswerk des DGB 60 (6), S. 36–37.

Hofstetter, Yvonne (2014): Sie wissen alles. Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen. 1. Aufl. München: Bertelsmann.

Horne, Christine; Darras, Brice; Bean, Elyse; Srivastava, Anurag; Frickel, Scott (2014 (online): Privacy, Technology, and Norms. The Case of Smart Meters. In: Social Science Research. DOI: 10.1016/j.ssresearch.2014.12.003.

Hubbard, Phil (2002): Thinking Geographically. Space, Theory and Contem- porary Human Geography. London, Continuum.

Hubig, Christoph; Koslowski, Peter (Hg.) (2008): Maschinen, die unsere Brüder werden. Mensch-Maschine-Interaktion in hybriden Systemen. Paderborn, Fink (Ethische Ökonomie, 11).

Jackson, Richard; Sinclair, Samuel Justin (Hg.) (2012): Contemporary Debates on Terrorism. London, Routledge.

Jaekel, Michael; Bronnert, Karsten (2013): Die digitale Evolution moderner Großstädte. Apps-basierte innovative Geschäftsmodelle für neue Urbanität. Wiesbaden, Springer Vieweg.

Jakubowski, Peter (2014): Auf dem Weg zu Smart Cities. Stadtzukünfte mit neuen Technologien. Bonn, BBSR.

Jason Reitman (2009): Up in the Air (Film). Paramount Pictures.

Joas, Hans (Hg.) (2007): Lehrbuch der Soziologie. 3. Aufl. Frankfurt am Main, Campus Verlag GmbH (Sozialwissenschaften 2001-2008).

Kaczorowski, Willi (2014): Die smarte Stadt – Den digitalen Wandel intelligent gestalten. Handlungsfelder Herausforderungen Strategien. Stuttgart, Richard Boorberg Verlag.

Kahl, Martin; Hegemann, Hendrik (2014): Debatte beendet? Die EU, Deutschland und die Antiterrorpolitik nach der NSA-Affäre. In: Friedensgutachten: Institut für Entwicklung und Frieden (INEF); Forschungsstätte der Evangelischen Studiengemeinschaft (FEST); Institut für Friedensforschung und Sicherheits- politik an der Universität Hamburg (IFSH); Hessische Stiftung Friedens- und Konfliktforschung (HSFK), S. 154–166.

Kammerer, Dietmar (2008): Bilder der Überwachung. Humboldt-Univ. Frankfurt am Main, Berlin.

Kammerer, Dietmar (2011): Das Werden der "Kontrolle". Herkunft und Umfang eines Deleuze'schen Begriffs. In: Nils Zurawski (Hg.): Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle. Opladen, Budrich UniPress, S. 19–34.

Kawashima, Kentaro (2008): Digitale Videokameras als neue Strategie der Überwachung. Drei Szenen aus Japan. In: Ralf Schnell und Karl Ludwig Pfeiffer (Hg.): Schwellen der Medialisierung. Medienanthropologische Perspektiven – Deutschland und Japan. Bielefeld: Transcript-Verl, S. 153–170.

Kehrt, Christian; Schüssler, Petert; Weitze, Marc-Denis (Hg.) (2011): Neue Technologien in der Gesellschaft. Akteure, Erwartungen, Kontroversen und Konjunkturen. Bielefeld, Transcript-Verl (Science studies).

Kemper, Peter; Mentzer, Alf; Tillmanns, Julika (Hg.) (2014): "Wir nennen es Wirklichkeit". Denkanstöße zur Netzkultur. Stuttgart Reclam (Reclam Taschenbuch, 20357).

Kitchin, Rob; Martin Dodge (2007), 'Rethinking Maps', Progress in Human Geography, 31 (2007), S. 331–44.

Kitchin, Rob (2013): Big Data and Human Geography. Opportunities, Challenges and Risks. In: Dialogues in Human Geography 3 (3), S. 262–267. DOI: 10.1177/2043820613513388.

Kitchin, Rob (2014): From a Single Line of Code to an Entire City: Reframing Thinking on Code and the City', 2014 http://papers.ssrn.com/sol3/papers.cfm? abstract_id= 2520435.

Klauser, Francisco Reto (2006): Die Videoüberwachung öffentlicher Räume. Zur Ambivalenz eines Instruments sozialer Kontrolle. Univ., Diss. Freiburg (Schweiz). Frankfurt am Main, Campus-Verl (Campus Forschung, 902).

Klein, Inga (2011): Überwachte Sicherheit oder sichere Überwachung? Kulturelle Deutungsmuster im Diskurs um den biometrischn Reisepass. In Zurawski, Nils (Hg.) (2011): Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle. Opladen, Budrich UniPress.

Kollek, Regine (2013): Ethik der Technikfolgenabschätzung in Medizin und Gesundheitswesen. Herausforderungen für Theorie und Praxis. In: Alexander Bogner (Hg.): Ethisierung der Technik – Technisierung der Ethik. Der Ethik-Boom im Lichte der Wissenschafts- und Technikforschung. Baden-Baden, Nomos, S. 199–214.

Koonings, Kees; Kruijt, Dirk (Hg.) (2007): Fractured Cities. Social Exclusion, Urban Violence and Contested Spaces in Latin America. London, Zed Books.

Krause, Thomas: Geschichte des Strafvollzugs. Von den Kerkern des Altertums bis zur Gegenwart. Darmstadt, WBG.

Kriminologisches Journal (2014): Themenheft Technologien der Verdachtsgewinnung, Vol. 46, Nr. 3.

Kurz, Constanze (2008): Biometrie nicht nur an den Grenzen. Erkennungsdienstliche Behandlung für jedermann, in: Gaycken, Sandro; Kurz, Constanze (Hg.) (2008): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript.

Künzli, Liz (2007): Bahnhöfe. Ein literarischer Führer. Frankfurt am Main, Eichborn.

Lacy, Mark (2014): Security, Technology and Global Politics. Thinking with Virilio. London, Routledge.

LaGory, Mark; Fitzpatrick, Kevin (2011): Unhealthy Cities. Poverty, Race, and Place in America. New York, Routledge.

Langheinrich, Marc; Mattern, Friedemann (2003): Digitalisierung des Alltags. Was ist Pervasive Computing? In: APUZ (42), S. 6–12.

Lannon, John (Hg.) (2013): Human Rights and Information Communication Technologies. Trends and Consequences of Use. Hershey, PA: Information Science Reference (Premier reference source).

Latour, Bruno (1991): Technology is Society Made Durable. In: John Law (Hg.): A Sociology of Monsters. Essays on Power, Technology and Domination, S. 103–131.

Latour, Bruno (2009): Wir sind nie modern gewesen. Versuch einer symmetrischen Anthropologie. Frankfurt am Main, Suhrkamp (Suhrkamp-Taschenbuch Wissenschaft : Stw).

Law, John (Hg.) (1991): A Sociology of Monsters. Essays on Power, Technology and Domination. The Sociological Review.

Leemans, Rik (Hg.) (2013): Ecological Systems. Selected Entries from the Encyclopedia of Sustainability Science and Technology. New York, NY, Springer.

Lefèbvre, Henri (1968): Le droit à la ville. Paris, Edition Anthropos.

Legnaro, Aldo; Birenheide, Almut (2008): Regieren mittels Unsicherheit. Regime von Arbeit in der späten Moderne. Konstanz: UVK. Online verfügbar unter http://deposit.d-nb.de/cgi-bin/dokserv?id=3116872&prov=M&dok_var=1&dok_ext=htm.

Leman-Langlois, Stephane (2013): Insecurity as an Engineering Problem. The Technosecurity Network. In: Kirstie Ball und Laureen Snider (Hg.): The Surveillance-Industrial Complex. A Political Economy of Surveillance. London, Routledge, S. 78–92.

Leman-Langlois, Stephane (Hg.) (2013): Technocrime, Policing and Surveillance. London, Routledge (Routledge frontiers of criminal justice, 3).

Lemke, Thomas (2005): Nachwort in Michel Foucault; Analytik der Macht. Frankfurt am Main, Suhrkamp.

Levan, Kristine; Mackey, David A. (Hg.) (2013c): Crime Prevention. Burlington, Mass, Jones & Bartlett Learning.

von Lewinski, Kai (2012): Zur Geschichte der Privatsphäre und Datenschutz – eine rechtshistorische Perspektive. In: Schmidt, Jan-Hinrik; Thilo Weichert (2012): Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bonn, BpB.

Löw, Martina (2001): Raumsoziologie. Frankfurt a. Main, Suhrkamp.

Löw, Martina (2008): Soziologie der Städte. Frankfurt a. Main, Suhrkamp.

Lüdtke, Alf; Wildt, Michael (Hg.): Staats-Gewalt: Ausnahmezustand und Sicherheitsregime. Historische Perspektiven. Göttingen, Wallstein.

Lyon, David (1988): The Information Society. Issues and Illusions. Cambridge: Polity.

Lyon, David (1994): The Electronic Eye. The Rise of Surveillance Society. Minneapolis, University of Minnesota Press.

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

Lyon, David (2002): Editorial. Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix. In: Surveillance & Society 1 (1), S. 1-7.

Lyon, David (2003): Fear, Surveillance and Consumption. In: The Hegdehog Review (Fall), S. 81–95.

Lyon, David (2003): Surveillance after September 11. Cambridge, Polity.

Lyon, David (2007): Surveillance Studies. An Overview. Cambridge, Polity.

Lyon, David (Hg. 2006): Theorizing Surveillance. The Panopticon and Beyond. Cullompton, Willan.

Lyon, David; Topak, Özgün E. (2013): Promoting Global Identification. Corporations, IGOs and ID Card Systems. In: Kirstie Ball und Laureen Snider (Hg.): The Surveillance-Industrial Complex. A Political Economy of Surveillance. London, Routledge, S. 27–43.

Mackey, David A. (2013c): Employing Surveillance in Situational Crime Prevention. In: Kristine Levan und David A. Mackey (Hg.): Crime Prevention. Burlington, Mass, Jones & Bartlett Learning, S. 209–226.

Mackey, David A. (c2013): The "X-Rated X-Ray". Reconciling Fairness, Privacy, and Security. In: Kristine Levan und David A. Mackey (Hg.): Crime Prevention. Burlington, Mass: Jones & Bartlett Learning, S. 227–236.

Maguire, Mark; Frois, Catarina; Zurawski, Nils; (Hg.) (2014): The Anthropology of Security: Perspectives from the Frontline of Policing, Counter-terrorism and Border Control. London, Pluto Press.

Mai, Manfred (2011): Technik, Wissenschaft und Politik. Studien zur Technik-soziologie und Technikgovernance. Wiesbaden: VS Verlag für Sozialwissen-schaften / Springer Fachmedien Wiesbaden GmbH Wiesbaden. Online verfügbar unter: http://dx.doi.org/10.1007/978-3-531-92763-3.

Mann, Steve; Nolan, Jason; Wellman, Barry (2002): Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. In: Surveillance & Society 1 (3), S. 331–355. Online verfügbar unter: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3344.

Marx, Gary T. (2002): What's New About the "New Surveillance"? Classifying for Change and Continuity. In: Surveillance & Society 1 (1), S. 9–29. Online verfügbar unter: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3391.

Marx, Gary T. (2005): Surveillance and Society. In: George Ritzer (Hg.): En-cyclopedia of Social Theory. Thousand Oaks/London, Sage.

Marx, Gary T. (2006): Varieties of Personal Information as Influences on Attitudes Toward Surveillance. In: Kevin D. Haggerty & Richard Ericson (Hg.): The New Politics of Surveillance and Visibility. Toronto, Toronto Univ. Press.

Masala, Carlo; Fischer, Susanne (2015): Innere Sicherheit nach 9:11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen? Wiesbaden, Springer VS.

Mathiesen, Thomas (2013): Towards a Surveillant Society. The Rise of Surveillance Systems in Europe. Hook, Waterside Press.

McCahill, Michael; Finn, Rachel L. (2014): Surveillance, Capital and Resistance. Theorizing the Surveillance Subject. London u.a., Routledge (Routledge studies in crime and society, 8).

McCahill, Mike (2002): The Surveillance Web. The Rise of Visual Surveillance in an English City. Cullompton, Willan.

Meyer, Adrian (2014): Hilfe, wo bin ich? In: Die Zeit, Nr. 49, 27. November 2014, S. 38.

Miles, Steven (2010): Spaces for Consumption. Pleasure and Placelessness in the Post-Industrial City. Los Angeles, Calif. [u.a.], SAGE.

Miller, Daniel (Hg.) (2005): Materiality. Durham, Duke Univ. Press.

Monahan, Torin (Hg.) (2006): Surveillance and Security. Technological Politics and Power in Everyday Life. London, Routledge.

Monahan, Torin & Tyler Wall (2007): Somatic Surveillance: Corporeal Control through Information Networks. In: Surveillance and Society, 4 (3), S. 154-173.

Monahan, Torin (2010): Surveillance in the Times of Insecurity. New Brunswick, Rutgers Univ. Press.

Monahan, Torin (2011): Surveillance as Cultural Practice. In: The Sociological Quarterly 52 (4), S. 495–508.

Monmonier, Mark S. (2004): Spying with Maps. Surveillance Technologies and the Future of Privacy. Pbk ed. Chicago, Ill, Univ. Chicago Press.

Morozov, Evgeny (2013): Smarte neue Welt. Digitale Technik und die Freiheit des Menschen. 1. Aufl., Blessing Verlag.

Möser, Kurt (2002): Die Geschichte des Autos. Frankfurt/Main, Campus.

Müller-Quade, Jörn (2014): Privatsphäre gesucht! Neue Big-Data-Techniken auf dem Vormarsch. Hamburg, Murmann.

Münkler, Herfried; Matthias Bohlender; Sabine Meurer (Hrsg. 2011): Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert. Bielefeld, transcript.

Nagenborg, Michael (2014): Ethik als Partnerin in der Technikgestaltung. In: Regina Ammicht Quinn (Hg.): Sicherheitsethik. Wiesbaden, Springer Fachmedien Wiesbaden GmbH (Studien zur Inneren Sicherheit, 16), S. 241–252.

Naik, Rohan; Lad, Kalpesh (2014): Challenges and Issues in Intelligent Video Surveillance System 3 (6), S. 2004–2011.

Nathanson, Stephen (2010): Terrorism and the Ethics of War, Cambridge, Cambridge University Press.

Nellis, Mike (2013): Surveillance, Stigma and Spatial Constraint. The Ethical Challenges of Electronic Monitoring. In: Mike Nellis (Hg.): Electronically Monitored Punishment. International and Critical Perspectives. London u.a., Routledge, S. 193–210.

Nellis, Mike (Hg.) (2013): Electronically Monitored Punishment. International and Critical Perspectives. London u.a., Routledge.

Neyland, Daniel (2009): Who's Who? The Biometric Future and the Politics of Identity. In: European Journal of Criminology 6, S. 135-155.

Nissenbaum, Helen (2004): Privacy as contextual integrity. Washington Law Review 79 (1), S. 119-158.

Norris, Clive; Armstrong, Gary (1999): The Maximum Surveillance Society. The Rise of CCTV. Oxford, Berg.

Norris, Clive; McCahill, Mike (2006): CCTV. Beyond Penal Modernism. In: British Journal of Criminology 46, S. 97-118.

Offenhuber, Dietmar; Ratti, Carlo (Hg.) (2013): Die Stadt entschlüsseln. Wie Echtzeitdaten den Urbanismus verändern. Gütersloh/Basel/Berlin, Brikhäuser/Bauverlag.

Paatz, Michael; Hilderink, Berthold (2010): Is Big Brother watching us? Datenschutz und ELENA. In: Arbeit und Arbeitsrecht. Die Zeitschrift für das Personal-Management 65 (Sonderausgabe), S. 48–51.

Pacione, Michael (2009): Urban Geography. A Global Perspective. Taylor & Francis. Online verfügbar unter: http://books.google.de/books?id=9-2lltgrYY8C.

Pavone, Vincenzo; Degli Esposti, Sara (2012): Public Assessment of New Surveillance-Oriented Security Technologies. Beyond the Trade-Off Between Privacy and Security. In: Public Understanding of Science 21 (5), S. 556–572. DOI: 10.1177/0963662510376886.

Popitz, Heinrich (1992): Phänomene der Macht. Tübingen, Mohr.

Price, Stuart (2012): Fesseln spürt, wer sich bewegt. Überwachung, Repression und Verfolgung im neoliberalen Staat. 1. Auflage, Hamburg, Laika Verlag (Edition Provo, 5).

Pridmore, Jason (2008): Loyal Subjects. Consumer Surveillance in the Personal Information Economy. Queens University,https://qspace.library.queensu.ca/bitstream/1974/1129/2/Pridmore_Jason_H_200804_PhD.pdf

Purenne, Anaik (2012): Police and surveillance in Paris: are the French police becoming knowledge workers and risk managers? In: Evelien van den Herrewegen; Gudrun Vande Walle; Nils Zurawski: Crime, Security and Surveillance. Effects for the Surveillant and the Surveilled. Den Haag, eleven.

Rekacewicz, Philippe (2013): Shoppen bis zum Abheben. In: Le Monde Diplomatique, 8.3.2013 (deutsch).

Rammert, Werner (2000): Technik aus soziologischer Perspektive 2. Kultur – Innovation – Virtualität. Wiesbaden, VS Verlag für Sozialwissenschaften. Online verfügbar unter: http://dx.doi.org/10.1007/978-3-322-87331-6.

Rammert, Werner (2007): Technik und Gesellschaft. In: Hans Joas (Hg.): Lehrbuch der Soziologie. 3. Aufl. Frankfurt am Main, Campus Verlag GmbH (Sozial-wissenschaften 2001-2008), S. 481-504.

Rammert, Werner (2008): Die Techniken der Gesellschaft. In Aktion, in Interaktivität und in hybriden Konstellationen. In: Karl-Siegbert Rehberg (Hg.): Die Natur der Gesellschaft. Verhandlungen des 33. Kongresses der Deutschen Gesellschaft für

Soziologie in Kassel 2006. Frankfurt am Main [u.a.], Campus-Verlag, S. 208–234.

Rammert, Werner (2008a): Die Macht der Datenmacher in der fragmentierten Gesellschaft. In: Sandro Gaycken; Constanze Kurz (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Transcript. S. 283–302.

Recki, Birgit (2013): Technik als Kultur. Plessner, Husserl, Blumenberg, Cassirer. In: Zeitschrift für Kulturphilosophie 7 (2), S. 287–303.

Rehberg, Karl-Siegbert (Hg.) (2008): Die Natur der Gesellschaft. Verhandlungen des 33. Kongresses der Deutschen Gesellschaft für Soziologie in Kassel 2006. Frankfurt am Main [u.a.], Campus-Verl.

Reichenbach, Gerold (2010): Risiko ist nicht gleich Risiko. In: Karlheinz Steinmüller; Lars Gerhold; Marie-Luise Beck (Hrsg. 2010): Sicherheit 2025. Forschungsforum Öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 10, September 2012, S. 197-115.

Rekacewicz, Philippe (2014): Endstation Shoppen. Ob Postamt, Bahnhof oder Flughafen – der öffentliche Raum verkommt zur Verkaufsfläche. In: Dorothee D'Aprile (Hg.): "Moloch, Kiez und Boulevard". Die Welt der Städte (Edition Le Monde diplomatique, 14), S. 10–11.

Renn, Ortwin (2011): Neue Technologien, neue Technikfolgen. Ambivalenz, Komplexität und Unsicherheit als Herausforderungen der Technikfolgenabschätzung. In: Christian Kehrt; Petert Schüssler; Marc-Denis Weitze (Hg.): Neue Technologien in der Gesellschaft. Akteure, Erwartungen, Kontroversen und Konjunkturen. Bielefeld, Transcript Verlag (Science studies), S. 63–76.

Rieger, Matthias (2015): Sicherheit als soziale Gefahr? Entpersonalisierende Sicherheitspraktiken an Flughäfen. In: Gerrit Herlyn; Nils Zurawski (Hg.): Achtung Sicherheitskontrollen! – Flughäfen, Kultur, Un/Sicherheiten. Münster, Lit.

Rinsen, James (2014): Pay any Prize – Greed, Power and Endless War. Houghton Mifflin Harcourt.

Rolf, Hauke Jan (2006): Urbane Globalisierung. Bedeutung und Wandel der Stadt im Globalisierungsprozess. Wiesbaden, Dt. Univ.-Verl.

Rolshoven, Johanna (2011): Mobilitätskulturen im Parkour. Überlegungen zu einer kulturwissenschaftlichen Mobilitätsforschung. In: Reinhard Johler; Max Matter; Sabine Zinn-Thomas (Hg.): Mobilitäten. Europa in Bewegung als Herausforderung kulturanalytischer Forschung. Münster.

Rosol, Christoph (2007): RFID. Vom Ursprung einer (all)gegenwärtigen Kulturtechnologie. Berlin, Kadmos.

Rule, James B.; Graham Greenleaf (Hrsg.2008): Global Privacy Protection. The first Generation. Cheltenham, Edward Elgar.

Rule, James B. (1974): Private Lives and Public Surveillance. Social Control in the Computer Age. New York, Shocken Books.

Samatas, Minas (2004): Surveillance in Greece. From Anticommunist to Consumer Surveillance. New York, Pella Publishing Co.

Samatas, Minas (2013): The SAIC-Siemens 'Super-Panopticon' in the Athens 2004 Olympics as a Case of 'McVeillance'. The Surveillance Industrial Complex's Unscrupulous Global Business. In: Kirstie Ball; Laureen Snider (Hg.): The Surveillance-Industrial Complex. A Political Economy of Surveillance. London [u.a.], Routledge, S. 61–77.

Schaefer, Kerstin (2015): Der ‚vergessene Passagier'. Eine ethnografische Fallstudie zum Thema Fliegen und Sicherheit. In: Gerrit Herlyn; Nils Zurawski (Hg.): Achtung Sicherheitskontrollen! – Flughäfen, Kultur, Un/Sicherheiten. Münster, Lit.

Scheerer, Sebastian (2000): Soziale Kontrolle – ein schöner Begriff für böse Dinge? In: Helge Peters (Hg.): Soziale Kontrolle. Zum Problem der Nonkonformität in der Gesellschaft. Opladen, Leske & Budrich.

Schewe, Christoph S. (2009): Das Sicherheitsgefühl und die Polizei. Darf die Polizei das Sicherheitsgefühl schützen? Berlin, Duncker & Humblot (Schriften zum öffentlichen Recht : SöR).

Schlepper, Christina, Christian Wickert, Judith Wöbcke & Bettina Paul (2015): „… das kennt man ja vom Flughafen". Über die Akzeptanz neuer Sicherheitsmaßnahmen im Fährverkehr2015. In Gerrit Herlyn; Nils Zurawski (Hg.): Achtung Sicherheitskontrollen! – Flughäfen, Kultur, Un/Sicherheiten. Münster, Lit.

Schmidt, Jan-Hinrik; Weichert, Thilo (2012): Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bonn, BpB.

Schmidt, Eric; Cohen, Jared; Neubauer, Jürgen (2013): Die Vernetzung der Welt. Ein Blick in unsere Zukunft. 1. Aufl. Reinbek bei Hamburg, Rowohlt. Online verfügbar unter: http://www.socialnet.de/rezensionen/isbn.php?isbn=978-3-498-06422-8.

Schnell, Ralf; Pfeiffer, Karl Ludwig (Hg.) (2008): Schwellen der Medialisierung. Medienanthropologische Perspektiven – Deutschland und Japan. Bielefeld, Transcript Verlag.

Schroer, Markus (2006): Räume, Orte, Grenzen. Auf dem Weg zu einer Soziologie des Raums. Frankfurt a. Main, Suhrkamp.

Schulzki-Haddouti Christiane (2014): Schädliche Daten-Emissionen: Wem Ihr Auto was über Sie verrät", erschienen im *"c't"-Magazin* 2014, Heft 19.

Simon, Bart (2005): The Return of Panopticism: Supervision, Subjection and the New Surveillance. In: Surveillance and Society, 3 (1), S. 1-20.

Simonis, Georg (2013): Konzepte und Verfahren der Technikfolgenabschätzung. Wiesbaden, Springer Fachmedien Wiesbaden.

Singelnstein, Tobias; Stolle, Peer (2008): Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert. Wiesbaden, VS (2. überarbeitete Auflage).

Soja, Edward W. (1989): Postmodern Geographies. The Reassertion of Space in Critical Social Theory. London, Verso.

Soja, Edward W. (1996): Thirdspace. Journeys to Los Angeles and Other Real-imagined Places. Malden/Oxford, Blackwell.

Spaaij, Ramón (2013): Risk, Security and Technology. Governing Football Supporters in the Twenty-First Century. In: Sport in Society 16 (2), S. 167–183. Online verfügbar unter: http://www.tandfonline.com/doi/abs/10.1080/17430437.2013.776249#.VRKU4-GoPPc.

Stalder, Felix (2002): Opinion. Privacy is not the antidote to surveillance. In: Surveillance and Society 1 (1), S. 120-124.

Stanley, Jay (2013): Police Body-Mounted Cameras. With Right Policies in Place, a Win For All. ACLU. Online verfügbar unter: https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all, zuletzt geprüft am 06.01.2015.

Staples, William G. (2014): Everyday Srveillance. Vigilance and Visibility in Postmodern Life. 2. Auflage, Lanham, Md u.a., Rowman & Littlefield.

Stark, Holger; Rosenbach, Marcel (2014): Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung. 1. Auflage, München, Dt. Verl.-Anst.

Steinmüller, Karlheinz; Gerhold, Lars; Beck, Marie-Luise (Hg.) (2010): Sicherheit 2025. Forschungsforum Öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 10, September 2012.

Steven Spielberg (2004): Terminal. Mit Tom Hanks. Dream Works.

Stolle, Peer; Singelnstein, Tobias (2012): Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert. Wiesbaden, VS Verlag für Sozialwissenschaften.

Stott, C.; Hoggett, J.; Pearson, G. (2012): 'Keeping the Peace'. Social Identity, Procedural Justice and the Policing of Football Crowds. In: British Journal of Criminology 52 (2), S. 381–399. Online verfügbar unter: http://bjc.oxfordjournals.org/content/early/2011/09/20/bjc.azr076.

Sugden, J. (2012): Watched by the Games. Surveillance and Security at the Olympics. In: International Review for the Sociology of Sport 47 (3), S. 414–429. Online verfügbar unter: http://irs.sagepub.com/content/47/3/414.

Surette, Ray (2005): The Thinking Eye. Pros and Cons of Second Generation CCTV Surveillance Systems. In: Policing 28 (1), S. 152–173. Online verfügbar unter: http://www.emeraldinsight.com/doi/abs/10.1108/13639510510581039.

Svenonius, Ola (2011): Sensitising Urban Transport Security. Stockholm University Press.

Taylor, Emmeline (2011): Awareness, understanding and experiences of CCTV amongst teachers and pupils in three UK schools. In: Information Polity. An International Journal of Government & Democracy in the Information Age 16 (4), S. 303-318.

Taylor, Emmeline (2013): Surveillance Schools; Security, Discipline and Control in Contemporary Education. Palgrave Macmillan, Basingstoke.

Thompson, Scott; Genosko, Gary (2006): Administrative surveillance of alcohol consumption in Ontario, Canada: pre electronic technologies of control. In Surveillance and Society, 4 (1/2), S. 29-51.

Thompson, Scott (2008): Separating the sheep from the goats: The United Kingdom‘s National Registration programme and social sorting in the pre-electronic era. In: Colin J. Bennett; David Lyon (Hg.): Playing the Identity Card. London/New York, Routledge.

Thompson. Scott (2014): Making Up Soldiers: The Role of Statistical Oversight and Reactive Path Dependence in the Effectiveness of Canada’s WWII Mobilization Program 1940-1943. In: Surveillance and Society 12 (4), S. 547-565.

Timan, Tjerk (2014). Surveillance in Urban Nightscapes. A STS-Informed Perspective. TECNOSCIENZA: Italian Journal of Science & Technology Studies 4(2), S. 93–124.

Townsend, Anthony M. (2014): Smart Cities. Big Data, Civic Hackers, and the Quest for a New Utopia. New York, NY, Norton.

Töpfer, Eric (2007): Videoüberwachung – eine Risikotechnologie zwischen Sicherheitsversprechen und Kontrolldystopien. In: Nils Zurawski (Hg.): Surveillance Studies. Perspektiven eines Forschungsfeldes. Opladen, Barbara Budrich.

Töpfer, Eric (2009): Videoüberwachung als Kriminalprävention? Plädoyer für einen Blickwechsel. In: Kriminologisches Journal 41 (4), S. 272–282.

Tudge, Robin (2011): The No-Nonsense Guide to Global Surveillance. Toronto, New Internationalist.

van der Ploeg, Irma (1999): The Illegal Body. „Eurodac“ and the Politics of Biometric Identification. In: Ethics and Information Technology 1, S. 295-302.

van der Ploeg, Irma (2006): Borderline Identities. The Enrollment of Bodies in the Technological Reconstruction of Borders. In: Torin Monahan (Hg.): Surveillance and Security. Technological Politics and Power in Everyday Life. New York/ London, Routledge.

Vannini, Phillip (2009): Material Culture and Technoculture as Interaction. In: Phillip Vannini (Hg.): Material Culture and Technology in Everyday Life. Ethnographic Approaches. New York u.a., Lang, S. 73–88.

Vannini, Phillip (Hg.) (2009a): Material Culture and Technology in Everyday Life. Ethnographic Approaches. New York u.a., Lang.

van Oijen, Charlotte; Bokhorst, Meike (2012): Securing the Legitimacy of Surveillance: Automatic Number Plate Recognition in Dutch Police. In: Evelien van den Herrewegen; Gudrun Vande Walle; Nils Zurawski (Hg.): Crime, Security and Surveillance. Effects for the Surveillant and the Surveilled. Den Haag, eleven.

Vasilache, Andreas (2012): Sicherheit, Entgrenzung und die Suspendierung des Privaten. In: Christopher Daase, Philipp Offermann und Valentin Rauer (Hg.): Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr. 1. Auflage, Frankfurt am Main, Campus Verlag (Sozialwissenschaften 2012), S. 133–158.

Virilio, Paul (2009): Der eigentliche Unfall. Wien, Passagen.

Volker Eick; Briken, Kendra (Hg.) (2013): Urban (In)Security. Policing the Neoliberal Crisis. Ottawa, Red Quill Books.

Volti, Rudi (2006): Cars and Culture. The Life Story of a Technology. Baltimore, John Hopkins University Press.

Vukelic, Tatjana (2015): Kulturelle Ähnlichkeiten und Differenzen bezüglich Sicherheitsmaßnahmen an den Flughäfen aus Passagiersicht. In: Gerrit Herlyn; Nils Zurawski (Hg.): Achtung Sicherheitskontrollen! – Flughäfen, Kultur, Un/Sicherheiten. Münster, Lit.

Wacquant, Loïc (2009): Bestrafen der Armen. Zur neoliberalen Regierung der sozialen Unsicherheit. Opladen, Budrich.

Wagenaar, Pieter; Boersma, Kees (2012). Zooming in on'heterotopia': CCTV-operator practices at Schiphol Airport. In: Information Polity 17 (1), S. 7-20.

Wagner, Katrin; Bonß, Wolfgang (2014): Risikobasiert versus One Size Fits All. Neue Konzepte der Passagierüberprüfung im Luftverkehr. Neubiberg, Universität der Bundeswehr München.

Warren, Adam; Bell, Morag; Budd, Lucy (2010): Airports, Localities and Disease: Representations of Global Travel during the H1N1 Pandemic. In: Health & Place 16, S. 727–35

Wassmann, Jürg; Dasen, Pierre R. (1998): Balinese Spatial Orientation. Some Evidence for Moderate Linguistic Relativity. In: The Journal of the Royal Anthropological Society (Man) 4 (4), S. 689-711.

Wassmann, Jürg (1993): The Yupno as Post-Newtonian Scientists. The Question of What is Natural in Spatial Descriptions. In: The Journal of the Royal Anthropological Society (Man) 29 (3), S. 645-666.

Weber, Max (1972): Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie. 5. Auflage, Tübingen, Mohr.

Webster, C. William R.; Töpfer, Eric; Klauser; Francisco R.; Raab, Charles D. (Hg.) (2012): Video Surveillance-Practices and Policies in Europe. Information and the Public Sector.

Wehrheim, Jan (2012): Die überwachte Stadt. Sicherheit, Segregation und Ausgrenzung. 3. Auflage, Opladen, Budrich.

Werlen, Georg (2009): Geographie/Sozialgeographie. In: Stephan Günzel (Hg.): Raumwissenschaften. Frankfurt a. Main, Suhrkamp.

Whitaker. Reg (1999): Das Ende der Privatheit. Überwachung, Macht und soziale Kontrolle im Informationszeitalter. München, Kunstmann.

White, Andrew (2014): Digital Media and Society. Transforming Economics, Politics and Social Practices. Basingstoke / Hampshire, Palgrave Macmillan.

Wiedemann, Gregor (2011): Regieren mit Datenschutz und Überwachung. Informationelle Selbstbestimmung zwischen Sicherheit und Freiheit. Marburg, Tectum-Verlag ([Wissenschaftliche Beiträge aus dem Tectum-Verlag / Reihe Politikwissenschaften] Wissenschaftliche Beiträge aus dem Tectum-Verlag).

Wiegandt, Claus-Christian (2014): „Erleben, was verbindet" – Neue Medien in der T-City in Friedrichshafen. Hemmnisse und Erfolgsbedingungen bei der Umsetzung eines Smart City-Konzepts. In: Thomas Christian Bächle und Caja Thimm (Hg.): Mobile Medien – mobiles Leben. Neue Technologien, Mobilität und die

mediatisierte Gesellschaft. Berlin, LIT (Bonner Beiträge zur Onlineforschung, 3), S. 245–270.

Wilson, Dean Jonathon; Serisier, Tanya (2010): Video Activism and the Ambiguities of Counter-Surveillance. In: S&S 8 (2), S. 166–180. Online verfügbar unter: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3484.

Winkelmann, Arne; Förster, Yorck (Hg.) (2007): Gewahrsam. Räume der Überwachung. [anlässlich der Ausstellung "Gewahrsam. Räume der Überwachung" … in Frankfurt am Main (21. April 2007 – 1. Juli 2007]. Deutsches Architekturmuseum (Frankfurt). Heidelberg, Kehrer.

Winner, Langdon (1980): 'Do Artifacts Have Politics?'. In: Daedalus, S. 121-136.

Wright, David; de Hert, Paul (Hg.) (2012): Privacy Impact Assessment. Heidelberg / London / New York, Springer.

Würtenberger, Thomas; Gusy, Christoph; Lange, Hans-Jürgen (Hg.) (2012): Innere Sicherheit im europäischen Vergleich. Sicherheitsdenken, Sicherheitskonzepte und Sicherheitsarchitektur im Wandel. Berlin u.a., LIT-Verlag (Zivile Sicherheit : Schriften zum Fachdialog Sicherheitsforschung).

Yalcin, Siddika Berna Ors (Hg.) (2010): Radio Frequency Identification. Security and Privacy Issues. 6th international workshop, RFIDSec 2010, Istanbul, Turkey, June 8-9, 2010; revised selected papers. RFIDSec; International Workshop on RFID Security. Berlin, Springer (Lecture notes in computer science, 6370).

Zerback, Ralf (2009): Metternichs IM. Wie Österreichs Staatskanzler Anfang des 19. Jahrhunderts den ersten modernen Überwachungsstaat in Deutschland schuf. In: Die Zeit, 10.06.2009 (25).

Zoche, Peter; Kaufmann, Stefan; Haverkamp, Rita (Hg.) (2011): Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. Bielefeld, Transcript Verlag (Sozialtheorie).

Zurawski, Nils (2005): „I know where you live!" – Aspects of watching, surveillance and social control in a conflict zone (Northern Ireland). In: Surveillance & Society 2 (4), S. 498-512.

Zurawski, Nils (2007): Quantitative Umfrage zu Videoüberwachung, Sicherheitsgefühl und Raumwahrnehmung an drei Standorten in Hamburg. Abschlussbericht.

Zurawski, Nils (Hg.) (2007a): Sicherheitsdiskurse. Angst, Kontrolle und Sicherheit in einer "gefährlichen" Welt. Frankfurt am Main u.a., Lang.

Zurawski, Nils (Hg.) (2007b): Vom öffentlichen Raum zu dessen Phantasie – cognitive mapping und die Überwachung öffentlicher Raume. Katalog zur Ausstellung: "Gewahrsam. Räume der Überwachung" im ehemaligen Polizeigefängnis Klapperfeld in Frankfurt. Heidelberg, Kehrer.

Zurawski, Nils (Hg.) (2007c): Surveillance studies. Perspektiven eines Forschungsfeldes. Opladen, Budrich.

Zurawski, Nils (2009): Videoüberwachung. Praktische Überlegungen zu einer allgegenwärtigen Technologie. In: Jürgen Scheele (Hg.): Medien, Macht und Demokratie. Neue Perspektiven. Berlin.

Zurawski, Nils (Hg.) (2011): Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle. Opladen, Budrich UniPress.

Zurawski, Nils (2011a): ‘Budni, ist doch Ehrensache!‘ – Kundenkarten als Kontrollinstrument und die Alltäglichkeit des Einkaufens. In: Nils Zurawski (Hg): Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle. Opladen, Budrich Unipress.

Zurawski, Nils (2014): Raum-Kontrolle-Weltbild. Raumvorstellungen als Grundlage gesellschaftlicher Ordnung und ihrer Überwachung. Opladen, Budrich Unipress.

Zurawski, Nils (2014a): Geheimdienste und Konsum der Überwachung. Essay. In: APUZ 64 (18-19), S. 14–19.

Zurawski, Nils (2014b): Consuming Surveillance. Mediating control practices though consumer culture and everyday life. In: André Jansson; Miyase Christensen (Hg.): Media, Surveillance and Identity: A Social Perspective. Frankfurt/New York, Peter Lang.

Zurawski, Nils (2014c): Kartographien des Risikos. Das Unbekannte und die imaginären Geografien der Sicherheit. In: Kritische Berichte 3, S. 67-76.

Zureik, Elia (2010): Colonialism, Surveillance, and Population Control. Israel/ Palestine. In: Elia Zureik; David Lyon; Yasmeen Abu-Laban (Hg.): Surveillance and Control in Israel/Palestine. Population, Territory and Power. London, Routledge.

Zwick, Detlev., and J. Denegri Knott (2009): Manufacturing Customers: The Database as New Means of Production, In: Journal of Consumer Culture 9, S. 221–47.