SANFTE ÜBERWACHUNG?
EINE UNTERSUCHUNG ZUR AKZEPTANZ VON DIGITALEN FINGERABDRUCKTECHNOLOGIEN IM ALLTAG

Universität Hamburg

Fakultät für Wirtschafts- und Sozialwissenschaften

Dissertation

Zur Erlangung der Würde der Doktorin/des Doktors der Wirtschafts- und Sozialwissenschaften

(gemäß der Promotionsordnung vom 24. August 2010)

vorgelegt von

Sylvia Kühne

aus Rostock

Hamburg, 2019

Vorsitzender der Prüfungskommission: Prof. Dr. Torsten Heinemann

Erstgutachterin: Prof. Dr. Susanne Krasmann

Zweitgutachter: Prof. Dr. Jan Wehrheim

Datum der Disputation: 10.04.2018

Inhalt

Abkürzungsverzeichnis IV

Abbildungs- und Tabellenverzeichnis V

Einleitung 1

1 Biometrie und Akzeptanz 12

1.1 Über Biometrie 12

1.1.1 Die Genese der Biometrie 13

1.1.2 Der Diskurs über Biometrie 20

1.1.2.1 Biometrie als Sicherheitstechnologie 21

1.1.2.2 Biometrie als Risikotechnologie 23

1.2 Über Akzeptanz 30

1.2.1 Akzeptanz als gesellschaftstheoretischer Schlüsselbegriff 31

1.2.2 Akzeptanzforschung: Konzeptionelle Zugriffe 34

1.2.2.1 Individuelle Akzeptanz 35

1.2.2.2 Gesellschaftliche Akzeptanz 36

1.2.3 Die Akzeptanz von Biometrie: Ein Blick in die Empirie 38

1.3 Akzeptanz beforschen 48

1.3.1 Kritisches zur Akzeptanz(-forschung) 48

1.3.1.1 Eine Kritik an ihrer konsensuellen Orientierung 49

1.3.1.2 Eine Kritik am normativen Impetus 52

1.3.1.3 Eine Kritik an den vermeintlich eindeutigen Konstellationen 58

1.3.2 Akzeptanz beforschen: Methodologische Überlegungen 60

2 Über die Studie zur Akzeptanz: Die Entwicklung der durchgeführten Arbeiten 68

2.1 Eine ‚Ethnografie' der Akzeptanz 70

2.1.1 Die Auswahl der Untersuchungssettings 71

2.1.2 Teilnehmende Beobachtungen 72

2.1.3 Qualitative Interviews mit Fingerabdruckgebern 75

2.2 Die Durchführung der Erhebungen 77

2.3 Die Analyse des Materials ... 90

3 Zu den Bedingungen der Akzeptanz ... 96

3.1 Vom Objekt her besehen: Eine interpretativ flexible Technologie ... 96

3.1.1 Heterogene Zwecke im sozio-technischen Setting ... 97

3.1.1.1 Eine bequeme Einrichtung im Alltag: Supermarkt & Videothek ... 97

3.1.1.2 Ein Kontroll- und Sicherheitsinstrumentarium: Arztpraxis & Schule ... 102

3.1.1.3 Ein bürokratisches Sicherheitsmerkmal: Einwohnermeldeamt ... 106

3.1.2 Eine ambivalente Technologie ... 110

3.1.3 Das Wissen vom Fingerabdruck ... 116

3.1.4 Zusammenfassende Überlegungen ... 120

3.2 Vom Subjekt her besehen: Motivlagen und Ambivalenzen ... 123

3.2.1 Nutzungsbedingungen zwischen Zwang und Freiwilligkeit ... 123

3.2.1.1 Kontroll- und Sicherheitsmotivationen ... 124

3.2.1.1.1 Sicherheitsvorsorge ... 124

3.2.1.1.2 Kontrollmotive ... 129

3.2.1.2 Ambivalenzen der Automatisierung ... 133

3.2.1.2.1 Nebeneffekte des Verfahrens ... 133

3.2.1.2.2 Abhängigkeit von Technik ... 136

3.2.1.3 Situative Erfordernisse ... 141

3.2.2 Ambivalenzmanagement ... 147

3.2.2.1 Relative Privatheit und Vorstellungen kontextueller Integrität ... 148

3.2.2.2 Vertrauensverhältnisse: Das Ausblenden der unheimlichen Möglichkeiten ... 155

3.2.2.2.1 Vorgängiges Vertrauen durch Vertrautheit ... 159

3.2.2.2.2 Bestätigtes Vertrauen durch Authentizität und soziale Billigung ... 164

3.2.2.2.3 Ausdrücklich vergebenes Vertrauen: Der Fingerabdruck als Gabe ... 167

3.2.3 Zusammenfassende Überlegungen ... 173

3.3 Akzeptanz im Verhältnis von Vertrauen und Misstrauen ... 176

3.3.1 Exkurs 1: Vertrauen in der Akzeptanzforschung zu Sicherheitstechnologien ... 177

3.3.2 Exkurs 2: Zum Zusammenhang von Vertrauen, Misstrauen und Biometrie ... 182

3.3.3 Grenzen des Vertrauens ... 187

3.3.3.1 Biometrie als Ausdruck von Misstrauen ... 188

3.3.3.2 Ambivalentes Vertrauen: Die Unzurechenbarkeit staatlichen Handelns ... 192

3.3.4 Zusammenfassende Überlegungen ... 194

4 Schluss ... 196

Literaturverzeichnis 208

Quellen 232

Anhang 235

Anhang A: Interviewleitfaden für Fingerabdruckgeber 235

Anhang B: Zusammenfassung 238

Anhang C: Liste der aus der Dissertation hervorgegangenen Veröffentlichungen 239

Erklärung über professionelle Promotionsbetreuung 240

Eidesstattliche Versicherung 241

Abkürzungsverzeichnis

AFIS	Automatisiertes Fingerabdruck-Identifizierungs-System
Arzt	Zahnarztpraxis
BMI	Bundesministerium des Innern
BKA	Bundeskriminalamt
BSI	Bundesministerium für Sicherheit in der Informationstechnik
CCC	Chaos Computer Club
ePass	Elektronischer Reisepass
Einwo	Einwohnermeldeamt
EURODAC	European Dactylographic System
FAR	Falschakzeptanzrate
FRR	Falschrückweisungsrate
I	Interviewer
Schul1	Schule 1 (Gymnasium)
Schul2	Schule 2 (Grund-, Haupt- und Realschule)
Sm	Supermarkt
Vid	24-Stunden- bzw. Automaten-Videothek

Abbildungs- und Tabellenverzeichnis

Abbildung 1: Ausschnitt aus der Struktur der Interviews (Kategoriensystem) 93

Tabelle 1: Wie bewerten die Bürger die folgenden Kontroll- und Überwachungstechnologien? 43

Tabelle 2: Zustimmung und Ablehnung der Maßnahmen 44

Tabelle 3: Bedrohung der Privatsphäre und Empfinden von Kontrollverlusten 46

Tabelle 4: Umfang der Erhebungen 84

Tabelle 5: Interviews im Setting Arztpraxis (Arzt) 84

Tabelle 6: Interviews im Setting Videothek (Vid) 85

Tabelle 7: Interviews im Setting Supermarkt (Sm) 85

Tabelle 8: Interviews im Setting Schule - Gymnasium (Schul1) 86

Tabelle 9: Interviews im Setting Schule - Grund-, Haupt-, Realschule (Schul2) 87

Tabelle 10: Interviews im Setting Einwohnermeldeamt (Einwo) 88

Tabelle 11: Interviews mit „Fingerabdrucknehmern“ 89

Tabelle 12: Glaube an einen vertrauenswürdigen Datenumgang durch die Behörden 179

Tabelle 13: Glaube an einen vertrauenswürdigen Umgang mit erhobenen Daten durch staatliche und nicht-staatliche Institutionen 180

Tabelle 14: Häufigkeiten der Antworten auf die Frage nach dem „Vertrauen in die Regierung“ 181

Einleitung

„Yet coercion at least has the virtue (if that's what it is) of letting the subject (or object) know what is happening." (Gary T. Marx 2006a: 44)

Als „Biometrie", etymologisch hergeleitet aus dem Griechischen βίος (bios, Leben) und μέτρον (metron, Maß), werden heute in der Regel Technologien bezeichnet, die mittels maschineller Erkennung körperlicher und auch habitualisierter Merkmale eines Menschen Identifikation oder Verifikation (Groebner 2004: 46), das heißt mittels mathematisch-statistischer Verfahren die Erfassung und Vergewisserung von Identitäten ermöglichen sollen. Reicht das Interesse an Biodaten und am Lesen körperlicher Charakteristika weit in die Geschichte zurück, etwa in Form von Autoren- oder Urkundenzeichen in prähistorischen bzw. frühgeschichtlichen Zeiten (vgl. hierzu z.B. Cole 2002: 60f., Lindenberg 1996: 287f.), haben biometrische Verfahren mit ihrem Versprechen von objektiver Wiedererkennung anhand als einmalig geltender körperlicher Merkmale bis heute nicht an Faszination verloren. Fingerabdruckverfahren etwa geht nicht nur eine lange Geschichte der Standardisierung von sowohl zivilen als auch polizeilichen Identifikationssystemen voraus (vgl. Cole 2002, Pugliese 2010, Groebner 2004). Mit digitalen Daten arbeitende Fingerabdrucksysteme haben in den vergangenen Jahren auch an alltagspraktischer Relevanz hinzugewonnen und in Deutschland seit 2001 innerhalb weniger Jahre den Status einer „Nischentechnologie" außerhalb ‚traditioneller' polizeilicher Anwendungen verloren (Petermann/Sauter 2002: 99ff.). Mit der Neubewertung der „Sicherheit in allen Lebensbereichen" (ebd.: 98) im Anschluss an die politischen Deutungen der Anschläge vom 11. September 2001 wurde ein in diesem Sinne neuer „Siegeszug der Winzigkeit" (Lindenberg 1996) zunächst mit der Integration von digitalisierten Fingerabdruckdaten in nationale Identitätsdokumente[1] beschritten. In den vergangenen Jahren wurden überdies auch nicht-staatliche, das heißt kommerzielle, Alltagsanwendungen biometrischer Verfahren in Deutschland erschlossen (vgl. Bitkom 2009): mittels Fingerabdruckerfassung lassen sich beispielsweise der Einkauf im Supermarkt, das Mittagessen in der Schulmensa bezahlen oder DVDs ausleihen. Damit ist die Technologie der Fingerabdruckerkennung in Deutschland nicht mehr länger nur auf die Registrierung bestimmter Personengruppen durch vorwiegend staatliche Akteure beschränkt.

Dass biometrische Daten nicht länger nur polizeilich erzwungen oder staatlich verordnet, sondern zunehmend ebenfalls freiwillig preisgegeben werden, provoziert die Frage danach, was

[1] Digitalisierte Fingerabdrücke sind in Deutschland seit 2007 obligatorischer Bestandteil des Reisepasses und können seit 2010 optional auch im RFID-Chip des Personalausweises gespeichert werden.

es mit dieser neuen Freiwilligkeit der Datenpreisgabe auf sich hat. An dieser Stelle setzte das von der Deutschen Forschungsgemeinschaft (DFG) geförderte Forschungsprojekt „Biometrie als ‚soft surveillance'. Zur Akzeptanz von Fingerabdrücken im Alltag"[2] an, aus dem heraus die vorliegende Arbeit entstanden ist, und das am Beispiel der Biometrie zu ergründen suchte, unter welchen Bedingungen Fingerabdrücke preisgegeben und neue Kontrolltechnologien akzeptiert werden. Es nahm Bezug darauf, dass die neue Freiwilligkeit bzw. Bereitwilligkeit personengebundene Daten preiszugeben in den sogenannten Surveillance Studies – einem Feld, welches sein Forschungsobjekt innerhalb der multiplen und komplexen soziotechnischen Praktiken der intentionalen Datenerfassung und -verwendung verortet – im Begriff der „soft surveillance" (Marx 2006a) ihren konzeptionellen Entwurf gefunden hat. Als Kern einer sich verändernden „Kultur der Kontrolle" (vgl. Garland 2001), in der vor allem die Wahrnehmung von Risiken zunehmend das gesellschaftliche „Sicherheitsbewusstsein" (Conze 2012: 454) prägt und sich Sicherheitsangebote, -formen und -zonen (Singelnstein/Stolle 2006: 78) vermehren, kennzeichne diese neue[3], namentlich „sanfte", Überwachung eine zunehmende Alltäglichkeit von Aufforderungen, sich freiwillig erweiterten Kontrollbefugnissen zu unterwerfen und/oder private Daten preiszugeben um beispielsweise Zugang zu öffentlich-physischen oder virtuellen Räumen, sozialen Netzwerken, Informationen und/oder Konsumangeboten zu erhalten. Die Streuung der Biometrie, das heißt von Verfahren, die die Erfassung und Vergewisserung von Identitäten ermöglichen sollen, in unterschiedlichste gesellschaftliche Zusammenhänge ist danach als eine exemplarische Praktik dafür zu verstehen, dass Überwachung, das heißt die fokussierte, systematische und routinierte Aufmerksamkeit für persönliche Informationen mit dem Ziel der Beeinflussung, des Managements und Schutzes (Murakami-Wood et al. 2006: 4), seit dem Ende des 20. Jahrhunderts vermehrt, und technologisch mediiert (vgl. Marx 1988), in alltäglichen Aktivitäten aufgeht.

Im Oxymoron „mandatory voluntarism" (Marx 2006a) ist der soziale Funktionsmechanismus dieser Kontrollstrategie eines „governing by freedom" (vgl. Garland 1997, Krasmann 1999, 2001) aufgefangen.[4] Unter dem ironischen Untertitel „Hey Buddy, Can You Spare a DNA?" – eine, mutmaßliche, Abwandlung eines der bekanntesten Lieder über die Große Depression in den USA von E. Y. Yip Harburg und Jay Gorney (vgl. Medina 2010) –, beschreibt der Na-

[2] An diesem Projekt (Laufzeit Oktober 2010-Dezember 2013) waren, neben der Autorin, als Projektleitung Susanne Krasmann und Fritz Sack, sowie Jan Wehrheim als Mitarbeiter beteiligt.

[3] Der hier verwendete Begriff einer neuen Surveillance ist, wenngleich Ausgangspunkt der markierten Veränderung, nicht identisch mit jenem der „new surveillance" (Marx 1988), mit dem in der Regel das Kontrollpotential der technischen Neuerungen selbst adressiert wird (vgl. ebd. 2015: 43).

[4] Allerdings beschreiben Ericson und Haggerty (1997: 436) schon Ende der 1990er Jahre einen im ästhetischen Design verschwindenden Zwangscharakter von Überwachungstechnologien.

mensgeber der „sanften Überwachung“, der amerikanische Soziologie-Professor Gary T. Marx (2006a: 37), wie seiner Beobachtung nach während eines Massengentests in den USA ein staatlich gesetzter Zwang kommunikativ in die Bitte um eine Geste der Wohltätigkeit verwandelt wird:

> „In Truro, Mass. at the end of 2004, police politely asked all male residents to provide a DNA sample to match with DNA material found at the scene of an unsolved murder. Residents were approached in a non-threatening manner (even as their licence plate numbers were recorded) and asked to help solve the crime.“

In dieser neuen Lesart von Überwachung – in der faktischer Zwang zunehmend hinter Wahlmöglichkeiten und selbstbestimmte Entscheidungen zurücktritt – korrespondiert die neue Freiwilligkeit der Datenpreisgabe mit Strategien der Responsibilisierung. Appelliert werde an das Eigeninteresse der Bürger[5] auch im Alltag sich vervielfältigende (Un-)Sicherheitslagen zu berücksichtigen. Bieten sich biometrische Technologien etwa regelmäßig auch als individuelle Lösung für Datenschutz- und -sicherheitsdefizite an, weil z. B. persönliche Geheimzahlen nicht länger vergessen oder ausgespäht werden könnten (Janke 2002: 205), sollen die Bürger dafür in ein technisches Potenzial investieren, das angesichts staatlicher wie auch privater Interessen an den Daten nahezu beliebig zur Kontrolle genutzt werden kann (vgl. Legnaro 2003: 297). Denn obwohl im Zusammenhang mit jener partizipativen Überwachung mitunter auch von einer „Demokratisierung der Überwachung“ (Haggerty/Ericson 2000: 618) die Rede ist, weil diese theoretisch nicht länger in dem von Michel Foucault (1998) beschriebenen zentralistischen Gefüge des Panoptismus aufgehe (vgl. ebd.: 617f., Loftus/Goold 2011: 276, Haggerty 2008: 38, Marx 2006b), sie bisweilen aufgrund ubiquitärer technologischer Verfügbarkeiten ein emanzipatorisches Potential – als Überwachung „von unten“ (vgl. zur „sousveillance“ z.B. Mann et al. 2003, in diesem Sinne auch Nayar 2015, Monahan 2010) – entfalte, wird der Alltäglichkeit der Datenpreisgabe gleichwohl das Potential der so entstehenden Datensammlungen gegenübergestellt, die über ihre Verknüpfung wirkmächtig werden. Gerade weil vor dem Hintergrund einer nahezu umfassenden Technisierung, Automatisierung und in jüngerer Zeit Digitalisierung, wie sie etwa unter dem Stichwort des „ubiquitären Computing“ (Mattern 2003) angedeutet wird, die Instrumentarien der Überwachung, zu denen auch ursprünglich klassische Sicherheits- und Kontrolltechnologien gehören, zunehmend im Alltag und zugleich in seinen Objekten wie etwa Autos, Mobiltelefonen, Gebäuden (vgl. Marx 2006a: 38ff.), und, im Fall der Biometrie, mithin im Körper verschwinden (vgl. Aas 2006,

[5] Für eine bessere Lesbarkeit wird in der vorliegenden Arbeit auf die Verwendung der weiblichen Form verzichtet, außer es sind explizit Frauen angesprochen.

Lyon 2001), gilt die neue Freiwilligkeit der Datenpreisgabe als elementarer Baustein innerhalb der sogenannten „surveillance assemblage“ (Haggerty/Ericson 2000).

In einer, diesem Verständnis nach, primär auf digitalen Daten basierenden, modular und netzwerkförmigen Organisation von Sensoren, Kameras und/oder Datenbanken erweitert sich nicht nur das Feld potentieller Überwachungsakteure. Es vervielfältigen sich auch die Möglichkeiten der Verknüpfung der so mitunter en passen entstehenden elektronisch verarbeitbaren Datenbestände und ihre nicht sichtbare, mitunter unabsehbare Nutzung zu Kontroll- oder ursprünglich nicht intendierten bzw. unautorisierten Zwecken, wie sie etwa unter dem Stichwort des „function creep“ diskutiert werden (vgl. z.B. Mordini 2009: 294ff.). Könnten etwa Strafverfolgungsinteressen und bestimmte Sicherheitsanforderungen eine solche sekundäre Nutzung von Daten, die ursprünglich zu anderen Zwecken erhoben wurden, nahelegen, stehen die neuen Alltagstechnologien im Allgemeinen und die Biometrie im Besonderen in dem Verdacht, dem „sanften Überwachungsstaat […] zuzuarbeiten“ (Strasser 2006: 23), wenn etwa die Aushebelung der informationellen Selbstbestimmung dadurch befürchtet wird, dass auch in Deutschland vorbehaltlich strafprozessualer Verbote „nahezu alles, was technisch möglich ist bzw. gespeichert vorliegt, auch eingesetzt bzw. ausgewertet“ wird (Eisenberg et al. 2005: 93, vgl. Strasser 2006: 24f.).[6] Bereits die bloße Existenz biometrischer Daten, so wird regelmäßig befürchtet, schaffe „Begehrlichkeiten und neue Potentiale zur ausufernden Überwachung der Bürger.“ (Kurz 2008: 108)

Ist die Rede von der neuen Freiwilligkeit der Datenpreisgabe gerade in Bezug auf eine Technologie, deren gesamtgesellschaftliche Einführung sich etwa noch im 20. Jahrhundert dem Vorwurf der überwachungsinspirierten „Volksdaktyloskopie“ resp. Kriminalisierung ausgesetzt sah – und damit auf Widerstand der Bürger zu stoßen riskierte (vgl. Meßner 2010: 14, ausführlich dazu ebd. 2015)[7] –, insofern im Kern von einer Beunruhigung getragen, dann, zum einen, deshalb, weil die „doppelte Unverfügbarkeit“ (Krasmann/Wehrheim 2013: 359)

[6] Obwohl die Datenerhebung für die vorliegende Arbeit zu diesem Zeitpunkt bereits abgeschlossen war, lassen sich die medial breit bekannt gewordenen sogenannten ‚Snowden-Enthüllungen‘ 2013 (vgl. Greenwald/MacAskill 2013, Gellman/Poitras 2013) über das bis dato geheim gebliebene Überwachungsprogramm „Planning Tool for Resource Integration, Synchronization, and Management“ (PRISM) der US-amerikanischen National Security Agency (NSA) als ein eindrücklicher Beleg für die Multifunktionalität der vielfältigen alltäglichen Datenproduktionen lesen, die sich auch in Deutschland in Überwachungspraxen einfügen lassen. Für Christian Fuchs (2015) etwa stehen sie im Kontrast zum Konzept einer „Demokratisierung der Überwachung“ und bilden demgegenüber einen Beleg gegen für das Fortbestehen der „centralized surveillance“ (8).

[7] „Manche wenden ein, die Verwendung der Daktyloskopie verletze das ethische Gefühl des Paßpetenten. Der Daktyloskopierte müsse sich wie ein Verbrecher vorkommen“, zitiert Daniel Meßner (2010: 14) den Münchner Kriminalisten und Autor des bis heute als Standardwerk geltenden Buchs „System und Praxis der Daktyloskopie“, Robert Heindl, der zur Verbesserung der erkennungsdienstlichen Arbeit vorschlug, die Fingerabdrücke aller Bürger in den Pass zu integrieren.

des Körpers bei der Datenerfassung angesichts der mit der Digitalisierung einhergehenden Möglichkeiten das Risiko unabsehbarer Möglichkeiten von Bestandsaufnahmen in sich trägt (ebd.). In diesem Zusammenhang wird eine Besorgnis nicht nur darüber geäußert, welche weiteren Informationen sich aus körperlichen Daten ableiten lassen. Mit der Einhegung des Körpers in maschinelle Identifizierungsprozeduren würden zudem einzelne körperliche Merkmale wie Minutien, das heißt jene Feinmerkmale wie Verzweigungen und Endungen der Papillarleisten in der Fingerlinienstruktur, als pars pro toto für das „absolute Individuum" (Kreissl/Steinert 2008: 271) definiert. Eine Identität die sich entlang rein statistisch begründeter Zuschreibungen konstituiere (vgl. Aas 2006, van der Ploeg 1999a) läuft jedoch den Freiheitsbedingungen von Individualität zuwider (Alterman 2003). Vor allem in dieser Hinsicht beunruhigt, zum anderen, dass die sich in der Gegenwart zunehmend herausgebildete Nähe von technisch vermittelten Kontroll- und Steuerungsmöglichkeiten[8] nicht mehr länger jene ausdrücklichen bürgerlichen Akzeptanzvorbehalte zu provozieren vermag, wie sie sich noch in den, vom Expertendiskurs aus entfaltenden, Boykottinitiativen (Berlinghoff 2013) mit „flächenbrandartigen Auswirkungen" gegen die „Verwaltungsautomation" und die Volkszählung (Hubert 1983: 258) Anfang der 1980er Jahren zeigten. Ist, aus dem öffentlich kommunizierten Unbehagen an der Technik heraus, mit dem sogenannten Volkszählungsurteil doch gerade „das Grundrecht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde erstmals höchstrichterlich als Verfassungsrecht anerkannt worden" (Schaar 2009: 5), so irritiert die neue Freiwilligkeit insbesondere deshalb, weil sie in den Verdacht einer „informationellen Selbstgefährdung" (Hermstrüwer 2016) der Bürger gerät. Der österreichische Philosoph Peter Strasser, der 2006 auf einem Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mahnende Worte anlässlich der geplanten Integration biometrischer Daten in die deutschen Ausweispapiere fand, formulierte gegen Ende seines Vortrages sein Unbehagen folgendermaßen:

> „Was sich daher ausbreitet, ist einerseits ein Gefühl, in nichttransparenter Weise immer mehr digitale ‚Abdrücke' des eigenen Lebens in immer mehr Speichern zu hinterlassen, wodurch im Gegenzug der Ruf nach einem effektiven Datenschutz zur Sicherung der Privatsphäre immer lauter wird. Andererseits jedoch scheint die Öffentlichkeit immer weniger abwehrend auf elektronische Überwachungsmethoden zu reagieren, soweit diese dazu dienen, die öffentliche Sicherheit zu gewährleisten." (19)

Statt einer sozial erwünschten Nicht-Akzeptanz (Lucke 1995: 63), das heißt einem öffentlich sichtbaren Missbehagen an der Technologie – von dem die wissenschaftliche Befasstheit mit der Akzeptanz ja gerade ihren Ursprung nimmt (vgl. ebd.: 38) und mit dem die Kenntnisnah-

[8] Bereits 1988 prägte Roger Clarke in diesem Zusammenhang den Begriff der „Dataveillance".

me der mit ihr einhergehenden Risiken zum Ausdruck gebracht würde –, wird die beobachtbare Nutzung des Verfahrens in einer Weise gedeutet, wonach die Gegenleistung, etwa ein von den Anbietern in Aussicht gestellter Mehrwert, z.B. Sicherheits- oder auch Bequemlichkeitsgewinne (vgl. Albrecht 2002: 93), einen damit einhergehenden Verlust von Freiheitsrechten (vgl. Albrecht 2008: 133f.) offenbar soweit überwiegt, dass selbst die Preisgabe körperlicher Daten und damit ein Kernbereich der Privatsphäre (vgl. Arendt 1999: 131) nicht als ein besonderer Eingriff empfunden wird.

Ist damit das Problem- und zugleich thematische Spannungsfeld skizziert, in dem die vorliegende Untersuchung verortet ist, dann ist zugleich angedeutet, dass Sicherheits- und Überwachungsdiskurse, ausgehend von Vorstellungen über das funktionale Wirken der Biometrie, allgemeine Begründungen und damit auch Akzeptabilitätskriterien für den Einsatz biometrischer, aber auch anderer mit digitalen Daten operierender, Technologien bereitstellen. Von diesen ausgehend scheinen auch die Motive für ihre Nutzung auf der Hand zu liegen: sei es die Verführung zum allgegenwärtigen Sicherheitsstreben in einer neuen Kontrollkultur (wie es implizit das Konzept der „soft surveillance“ nahelegt, vgl. in diesem Sinne auch z.B. Legnaro 2011: 195f.), und/oder es wird eine schlichte Sorglosigkeit angesichts der mit der Technologie einhergehenden (technischen) Sicherheitsrisiken unterstellt (so, mit Bezug auf die Verbreitung von Web 2.0-Technologien, argumentierend etwa Heesen 2008: 241). Die Nutzung von Technologien, die eine Gefährdung der Privatsphäre riskieren können, scheine zudem gleichsam auf einen Bedeutungsverlust dieser selbst zu verweisen (ebd.). Vergleichbares deutet dann auch die Forschung zur Akzeptanz von Biometrie an. Diese, in der Regel mittels standardisierter Befragungen durchgeführten, Untersuchungen erheben vor allem Kosten-Nutzen-Erwartungen und grundsätzliche Einstellungen gegenüber unterschiedlichen staatlichen Überwachungstechnologien (vgl. z.B. Lüdemann /Schlepper 2013) oder lösen jene Vor- und Nachteile, z.B. des elektronischen Reisepasses (ePass), projektiv in Modellen wie dem „Price of Convenience“ (vgl. Ng-Kruelle et al. 2006) auf.

Dieser Forschung liegt allerdings ein technisch reduziertes Verständnis von Akzeptanz zugrunde und dies vor allem deshalb, weil sie Akzeptabilitätskriterien zum Maßstab der Akzeptanz macht, die wiederum in Sicherheits- und Überwachungsdiskursen bereitgestellt werden. Auf diese Weise lassen sich zwar Aussagen darüber treffen, welcher Risikograd einer Technologie im Fluchtpunkt einer zu bestimmenden „ethischen Verantwortbarkeit“ (Renn 2005: 29) akzeptabel ist. Woran sich der konkrete Umgang mit der Technologie aber tatsächlich orientiert bleibt in einer solchen Konzeption gleichwohl offen. Die der Einleitung vorangestellte resignative Einschätzung von Gary T. Marx (2006a: 6), die er in seinem ‚soft sur-

veillance-Aufsatz‘ trifft, dass zumindest der Vorzug des Zwangscharakters von Überwachung darin gelegen habe, dass klar gewesen sei, was eigentlich vor sich gehe, soll für die vorliegende Untersuchung dann auch so gelesen werden, dass dementsprechend nicht nur Klärungsbedarf hinsichtlich der Bedingungen von Akzeptanz besteht, sondern auch dahingehend, was der Begriff der Akzeptanz überhaupt bedeuten kann. So ist nämlich mit Blick auf die Akzeptanzforschung insgesamt auch ein theoretisches Defizit darin zu sehen, dass in diesem Feld – vorrangig betrieben von der Techniksoziologie (Risikoabschätzung) oder im Rahmen der wirtschaftswissenschaftlichen Verwendungsforschung – zwar keine umfassende Theorie der Akzeptanz zu identifizieren ist, sich das Verständnis von ihr gleichwohl regelmäßig auf die Verhaltensebene – als Ausdruck faktischer Akzeptanz – bezieht, deren Gründe dann in spezifischen Einstellungen gesucht werden.

Mit dem Vorhaben dieser Studie, die Irritation über die neue Freiwilligkeit der Preisgabe biometrischer Daten ebenfalls als eine Frage nach der Akzeptanz aufzugreifen, verbindet sich allerdings ein anderer Zugang. Ausgehend von einem Verständnis der Akzeptanz als interpretativem und aktivem Vorgang (vgl. Lucke 1995) wird argumentiert, dass, wenngleich gesellschaftliche Normen einen Bezugsrahmen für das zu Akzeptierende bieten können (ebd.: 99), Akzeptanz „nur in vergleichsweise wenigen Fällen […] gegenständlich, thematisch oder personell vorentschieden und dadurch weitestgehend determiniert“ ist (ebd.: 119f.). Sie wäre damit weder direkt aus der Technologie selbst, noch aus subjektiven Einstellungen der Nutzer ableitbar, sondern konstituiert sich erst im Verhältnis von *Subjekt* – *Objekt* – im jeweiligen *Kontext* (ebd.: 88ff.). Der im Projekt gewählte methodische Ansatz von Beobachtungen von Registrierungsprozessen und qualitativen Interviews mit Nutzern in unterschiedlichen Anwendungssettings: einer Arztpraxis, einem Supermarkt, einer Automatenvideothek, Schulen sowie behördlichen Anwendungen der ePass- und Personalausweisstellung, orientierte sich insofern an einem Verständnis von Akzeptanz als einer aktiven Aneignung der Fingerabdrucktechnologie durch in verschiedenen Kontrollregimen Handelnden. Statt von einer beobachtbaren Nutzung der Technologie auf die individuellen Nutzungsmotive der Nutzer zu schließen – etwa in Abhängigkeit davon, mit welchen Begründungen die jeweilige Anwendung beworben wird – wurde erwartet, dass die Be-Deutung von Biometrie und ihre Akzeptanz, in Anlehnung an interaktionstheoretische Überlegungen, erstens, durch die rechtliche und technische Ausgestaltung der konkreten Anwendung (vgl. Hornung 2005: 420) und das „Wissen“ (Berger/Luckmann 1980) der beteiligten Akteure darüber variiert, sowie, zweitens, in symbolischen Interaktionen hergestellt (vgl. Blumer 2004) wird. Obwohl dies dann auch heißt, dass sich die Bedeutung einer Technologie wie des Fingerabdruckverfahrens kaum vor-

ab bestimmen lässt, bildeten diskursimmanente Deutungsmuster, das heißt dominante Bestimmungen der Technologien im öffentlichen Diskurs, wie Überwachung vs. Sicherheit, Gefährdungen vs. Schutz der Privatsphäre, Degradierung vs. Distinktionsgewinne, gleichwohl den Ausgangspunkt des Forschungsprojektes. So lautete die These, dass die Akzeptanz von ihrer jeweils im Anwendungssetting interaktiv ausgehandelten Relevanz abhängig sei, denn nur mit ihrer situationsangemessenen Inszenierung, so die Annahme, könnten sich digitale Fingerabdrucksysteme als marktfähige Alltagstechnologie etablieren. In der vorliegenden Untersuchung werden diese Spannungsfelder demgegenüber allerdings als Akzeptabilitätskriterien verstanden, deren Bedeutung für die Akzeptanz es erst noch zu untersuchen gilt.

Vor diesem Hintergrund erfolgt, neben der Beantwortung der Fragen, welche Bedeutung die Fingerabdrucktechnologien in unterschiedlichen Anwendungssettings entfaltet und wie Motive ihrer Nutzung zu rekonstruieren sind, eine Einordnung der Akzeptanz, die sich, folgt man Doris Lucke (1995: 74ff.), im Horizont von aktiver Annahme oder passiver Hinnahme, von bewusster Zustimmung oder eher impliziter Übernahme bis hin zu widerwilliger Hinnahme, erzwungenem Einverständnis und Widerständigkeit bewegen kann. Ausgehend von dem überwachungstheoretischen Problemhintergrund betritt die Untersuchung dann auch ein noch vergleichsweise neues Terrain in den Surveillance Studies. Denn obwohl mit der zunehmenden Verbreitung der Biometrie auch in alltägliche Zusammenhänge die Auseinandersetzung mit der partizipativen Überwachung im Allgemeinen und der Biometrie im Besonderen in den Surveillance Studies bzw. ihnen zugeordneten Arbeiten zu einem reichhaltigen Literaturfundus geführt hat, stellte sich die Frage ihrer Akzeptanz (als ein interpretativer und aktiver Vorgang) lange Zeit nicht. Es dominierten mit Blick auf die Bedeutsamkeit neuer (Kontroll-)Technologien vor allem makrosoziologische Forschungen und Kernthemen waren vor allem ihre Genese (vgl. z.B. zur Fingerabdrucktechnologie Cole 2002) und ihre Folgen für Konzepte wie beispielsweise Privatheit (vgl. z.B. van der Ploeg 2003a, 2003b, Zureik 2010) oder Identität (Aas 2006, Mordini 2009, Neyland 2009). In den Mittelpunkt der Analyse gerückt sind zudem Logiken der Ordnung von Datenbeständen (vgl. z.B. Lyon 2007, Aas 2004). Diskutiert werden unter anderem die in Technik eingeschriebenen Kategorisierungen und die Folgen daraus abgeleiteten Kontrollhandelns hinsichtlich ihres Diskriminierungs- und Exklusionspotentials für bestimmte Bevölkerungsgruppen (vgl. z.B. Lyon 2007, Aas 2011). Biometrische Technologien werden folglich primär dahingehend kritisch in Augenschein genommen, wie sie sich in gesellschaftliche Logiken der Macht einfügen und diese ihrerseits erzeugen und mithin wie sich die Disziplinarlogik als Teil des panoptischen Prinzips, wie sie Michel

Foucault 1998 in „Überwachen und Strafen“ beschreibt, in immer neue Felder verbreitet.[9] Der so in gewisser Weise im doppelten Sinne ‚panoptische Blick‘ der Surveillance Studies hat dabei kaum Raum für das Subjekt selbst gelassen. Angesichts des dominanten Bezuges auf die Foucaultschen Gedanken ist dies insofern erstaunlich, als dass dieser selbst etwa mit der Frage „Was ist Kritik“ (1992) der unmündigen Haltung der passiven Subjekte jene kritische Haltung gegenüberstellt, in der das Subjekt „sich das Recht herausnimmt, die Wahrheit auf ihre Machteffekte hin zu befragen und die Macht auf ihre Wahrheitsdiskurse hin.“ (ebd.: 15) So regt sich unter überwachungstheoretischen Gesichtspunkten seit einigen Jahren dann auch eine Kritik gegen einen solchen Entwurf von „docile bodies“ (Kitchin/Dodge 2011 zit. in McCahill/Finn 2014: 4), das heißt von der Macht unterworfenen Subjekte (vgl. Yar 2003, Ball 2009, McCahill/Finn 2014). Statt als Bürger die „subject to surveillance“ sind, geraten diese zunehmend auch als „subjects of surveillance“ in den Blick (Lyon 2007: 7, Herv. i.O.). In diesem Zusammenhang fordern dann auch David Murakami Wood und William Webster (2009: 259f.) den Blick der Surveillance Studies auf die Überwachung als Normalität neu zu befremden und die Prozesse der alltäglichen Auseinandersetzung damit, was die „black box“ Überwachung verbirgt, zu ergründen:

> „Underpinning our argument is the simple proposition that technologically mediated surveillance practices raise significant questions about modern society, the nature of liberty and its relationship to security, and about relations between citizens, businesses and the state. Furthermore, a closer examination of the new ‘normality’ of everyday surveillance highlights the differentiated and diverse application of surveillance in modern European society.“ (ebd.: 260)

Wenn also, wie Gary T. Marx im Jahr 2005 (362) kritisierte, der Rede über Überwachungstechnologien eine adäquate Sprache fehle, um Überwachung zu diskutieren, dann lässt sich eine solche Kritik vor allem auf die Tatsache beziehen, dass das Eindringen des panoptischen Prinzips in immer neue Bereiche keinesfalls reibungslos von statten geht (vgl. auch Haggerty 2008: 34). So soll mit der Studie auch ein geforderter Beitrag zur qualitativen Forschung in den Surveillance Studies, im Sinne eines „returning to the things themselves“ (Friesen et al. 2009), der die subjektive Wahrnehmung von Überwachung einbezieht, geleistet werden.

Vor diesem Hintergrund gliedert sich die Arbeit im Einzelnen wie folgt:

[9] Disziplin ist dabei „ein Typ von Macht; eine Modalität der Ausübung von Gewalt; ein Komplex von Instrumenten, Techniken, Prozeduren, Einsatzebenen, Zielscheiben; sie ist eine ‚Physik‘ oder eine ‚Anatomie der Macht, eine Technologie“ (Foucault 1998: 276f.). Das panoptische Prinzip, „gesehen [zu werden], ohne selber zu sehen“ (ebd.: 257), das Foucault exemplarisch im Gefängnisentwurf Jeremy Benthams identifiziert, überträgt sich in den „Disziplinargesellschaften“ des 18. und 19. Jahrhunderts in die unterschiedlichsten Institutionen und ermöglicht der verwaltenden Macht in einer „ununterbrochenen, erschöpfenden, allgegenwärtigen Überwachung“ ihre Anforderungen von Normierung und Normalisierung durchzusetzen, ohne diese sichtbar zu machen oder gar selbst sichtbar zu sein (ebd.: 275).

Im ersten Kapitel wird das Verhältnis von Biometrie und Akzeptanz diskutiert. Hierzu wird in einem ersten Schritt das Werden des Fingerabdruckverfahrens im Hinblick auf seine gegenwärtige Relevanz auf der Basis des Forschungsstandes nachvollzogen. Rekapituliert werden sowohl seine Genese als auch seine diskursive Verortung und die hier verhandelten Akzeptabilitätskriterien. Da es zudem eine thematische Einführung zur ‚Alltagsbiometrie', im Besonderen des Fingerabdruckverfahrens, bildet, liegt der Schwerpunkt der Darstellungen des ersten Teils in zeitlicher Hinsicht vor allem auf der Einführung der Technologie um die letzte Jahrtausendwende. Daran schließen sich eine Auseinandersetzung mit dem Konzept der Akzeptanz sowie eine Darstellung des rudimentären Forschungsstandes zur Akzeptanz von Biometrie an. Zunächst wird nachvollzogen, wie die gesellschaftliche und wissenschaftliche Befasstheit das Verständnis von Akzeptanz entlang öffentlichen Konflikts aus modernisierungstheoretischer Hinsicht geprägt hat sowie welche theoretischen und empirischen Konzeptualisierungen sich daraus im Allgemeinen und im Besonderen für Untersuchungen, die die Akzeptanz neuer Technologien der Sicherheit und Kontrolle in den Blick nehmen, ergeben. Einer daran entfalteten Kritik an der Akzeptanzforschung folgen dann methodologische Überlegungen. Diskutiert wird, wie Akzeptanz verstanden werden und sich die Materialität der Technologie soziologisch mittels qualitativer Forschung erfasst lässt. Daran schließt sich im zweiten Kapitel die Beschreibung der Methodik des Forschungsprojektes an. Neben der Begründung der jeweils verwendeten Methoden vermittelt die Schilderung der konkreten Durchführung der Erhebungen erste empirische Einblicke in die untersuchten Anwendungssettings. Nachvollzogen werden in diesem Kapitel dann auch jene Modifikationen der Analyseperspektive, die sich im Verlauf der Untersuchung im Hinblick auf die Ausgangsannahmen des Projektes ergaben. Das dritte Kapitel widmet sich der Explikation der empirischen Ergebnisse der Untersuchung zu den Bedingungen der Akzeptanz. Dabei werden zunächst die sich aus dem variierten Fokus ergebenden Einsichten in die Bedeutungsebenen des Objektes Fingerabdrucktechnologie dargestellt. Es wird gezeigt, dass diese die Technologien nicht nur als vielfältig verwendbare, sondern auch in ihrer Bedeutung als ambivalent ausweisen. Auf der Basis dieser, auch als Einführung in die konkreten Untersuchungsfelder angelegten, Darstellung wird der Frage nachgegangen, auf welche Bezugspunkte die unterschiedlichen Bedeutungen der Fingerabdrucktechnologie verweisen. Hierfür wird die Rolle settingspezifischer und diskursimmanenter Deutungsrahmen ebenso diskutiert, wie die Rolle des Wissens, das sich entlang des Fingerabdruckverfahrens selbst entfaltet und für eine Konzeptualisierung des Akzeptanzhandelns in den Blick genommen. In einem weiteren Schritt wird im zweiten empirischen Unterkapitel die Frage nach den Nutzungsmotivationen in Relation zu den Bedingungen von

Freiwilligkeit und Zwang gesetzt und die herausgearbeitete Differenz zwischen tatsächlicher Fingerabdruckabgabe einerseits und kritischem Räsonnement andererseits für eine Einschätzung der Akzeptanzbedingungen herangezogen, um Aussagen zu den moderierenden Bedingungen der Akzeptanz zu treffen. Ausgehend von der hier dargestellten Relevanz von Vertrauensverhältnissen als Bedingung von Akzeptanz wird anschließend das Verhältnis von Kontrolle, Misstrauen und den Grenzen von Vertrauen für Fragen der Akzeptanz der Fingerabdrucktechnologie eingehender betrachtet. Im letzten Kapitel werden die zentralen Befunde dieser Arbeit zusammengefasst, auf der Basis der Untersuchungsergebnisse ein Vorschlag zur Akzeptanztypologie unterbreitet, sowie sich daraus ergebende Einsichten für zukünftige Akzeptanzforschungen abgeleitet.

1 Biometrie und Akzeptanz

In diesem Kapitel stehen die zentralen Begrifflichkeiten – Biometrie und Akzeptanz – und ihr Verhältnis zueinander im Mittelpunkt. Es wird dem, sowohl im öffentlichen als auch im wissenschaftlichen Diskurs, formulierten Unbehagen an der neuen Freiwilligkeit der Datenpreisgabe gefolgt und insofern der Blick auf die Krise der sozial erwünschten Nicht-Akzeptanz (Lucke 1995: 63) gerichtet. Krisen, so konstatierten Krasmann et al. (2014: 9 mit Bezug auf Koselleck 1982: 648f.), konturieren sich mit der Wahrnehmung einer Neuheit, „die aber noch im Übergang ist […] und gehen mit Unruhen oder Verunsicherungen einher, weil das Alte so nicht mehr gilt, das Neue aber noch nicht gefunden ist." Dieses ‚Alte' wird daher zunächst in Bezug auf die Bedeutung der Biometrie im wissenschaftlichen und öffentlichen Diskurs nachvollzogen. Es werden insofern unterschiedliche Akteure in den Blick genommen, die an der Konstruktion des Wissens über Biometrie beteiligt sind. In einem zweiten Schritt werden der Begriff der Akzeptanz und der Zugriff der Forschung auf das Konzept selbst untersucht. Vor dem Hintergrund einer Kritik an der gegenwärtigen Akzeptanzforschung werden die sich im Diskurs über Biometrie andeutenden Akzeptanz- und Akzeptierbarkeitserwartungen diskutiert, der sich methodologische Überlegungen darüber anschließen, was Akzeptanz überhaupt bedeuten und wie sie für eine empirische Erfassbarkeit der Akzeptanz von digitalen Fingerabdruckverfahren im Rahmen dieser Studie – im Sinne des Findens des ‚Neuen' – handhabbar gemacht werden kann.

1.1 Über Biometrie

Im Mittelpunkt der nachfolgenden Ausführungen steht die Relevanz der Biometrie. Die Darstellungen orientieren sich zunächst daran, warum Fragen der Identifikation aus einer historischen Perspektive überhaupt erst aufgekommen sind, welche Rolle hierfür körperliche Merkmale spielen und wie sich der Fingerabdruck selbst als ein kollektives Zeichen des Identitätsbeweises verbreiten und das Fingerabdruckverfahren in seiner Bedeutung als Identifizierungstechnik stabilisieren konnte. Als Antworten weist die Forschung sowohl soziale, politische und technologische Faktoren aus, sodass sich daraus eine theoretische Gemengelage unterschiedlicher Forschungsperspektiven ergibt, welche sowohl die Relevanz körperlicher Merkmale im Kontext systematischer Identifizierungspraktiken seit dem Mittelalter (vgl. z.B. Groebner 2004, Pugliese 2010) berücksichtigen, die (Weiter-)Entwicklung letzterer im Zuge einer kriminologischen Verwissenschaftlichung (vgl. z.B. Becker 2005) und zunehmenden Techni-

sierung der kriminalpolizeilichen Arbeit seit dem 19. Jahrhundert (vgl. ebd., Meßner 2015), als auch die Vereinnahmung der Technologie in spezifische Wissenskulturen und Technisierungsprozesse verfolgen (vgl. z.B. Cole 2002, 2005, Strasser 2005, Gates 2005, Pugliese 2010, Meßner 2015). Diese Entwicklungen werden nachfolgend skizziert, bevor der Blick in die Gegenwart schnellt und die Verbreitung des Fingerabdruckverfahrens in Deutschland seit der letzten Jahrtausendwende umrissen wird, für die sich vor allem das Zusammentreffen von technopolitischen und Sicherheitsdiskursen (vgl. Lyon 2001, Ceyhan 2008, Magnet 2011, Muller 2010, 2011, Kühne/Schlepper 2018, Kühne/Wehrheim 2013) als eine grundlegende Bedingung identifizieren lässt. Daran anschließend werden mit Blick auf den gegenwärtigen Diskurs die dominanten Diskussionslinien rund um das Fingerabdruckverfahren eruiert und entlang der darin verhandelten Vor- und Nachteile der Technologie dargestellt.

1.1.1 Die Genese der Biometrie

Die Genese biometrischer Verfahren lässt sich kaum auf einen kulturhistorischen Verweis der Verwendung biometrischer Zeichen als Autoren- oder Urkundenzeichen in prähistorischen bzw. frühgeschichtlichen Zeiten reduzieren (vgl. Lindenberg 1996, Cole 2002, Pugliese 2010, Meßner 2015). Gegenwärtig eingesetzten Fingerabdrucktechnologien geht vielmehr eine lange Geschichte der Standardisierung von sowohl zivilen als auch polizeilichen Identifikationssystemen voraus (vgl. Pugliese 2010: 25ff., Cole 2002, Gates 2005, Groebner 2004). Obzwar sich erst gegen Ende des 19. Jahrhunderts die Daktyloskopie (griechisch: daktylos „Finger“ und skopein „betrachten“) als polizeiliches Instrument der Wiedererkennung etabliert, macht etwa die Untersuchung Valentin Groebners (2004: 143), der die Anfänge einer Erfassung körperlicher Merkmale zum Zwecke der Identifizierung bis in die frühmoderne Anfertigung von papierenen Identitätsbeschreibungen zurückverfolgt, deutlich, dass bereits bevor der Fingerabdruck selbst zu einem Merkmal der Individualisierung wird, der Zugriff auf den Körper Bestandteil der Geschichte des administrativen Identifizierens ist. Eine im Verlauf des Mittelalters beginnende und mit dem 18. Jahrhundert zunehmend umfassender werdende schriftliche Registrierung körperlicher, sowie weiterer als individuell erachteter, Merkmale in Ausweisen, Pässen und Steckbriefen und der Abgleich dieser mit (internen) Registern (ebd.: 156, Cole 2002: 16) gelten als Ausdruck eines zunehmenden hoheitlichen Wissensbedürfnisses, unter Bedingungen anwachsender Mobilität und Anonymität Zurechenbarkeit und Eindeutigkeit von Identitäten herzustellen (Groebner 2004: 144, Gates 2006: 421, Lyon 2001: 35) und

mithin den sich zunehmend differenzierenden Gesellschaftskörper lesbar und damit regier- und kontrollierbar zu machen (Cole 2002: 3, vgl. Scott 1998).

Das Festmachen von Merkmalen an einer Person ist ein Akt der Individualisierung und mit Transkriptionen körperlicher Merkmale wird die Komplexität von Identität eingehegt (vgl. Groebner 2004: 86ff., Pugliese 2010: 27). Vor allem die Haut, so Groebner (ebd.: 75), wird „Gedächtnis" und ihre Besonderheiten, neben anderen körperlichen Merkmalen, zunehmend auf das Papier übertragen. Spätestens seit dem 18. Jahrhundert gelten für den sich langsam etablierenden Blick der Experten ihrer Zeit körperliche Merkmale als besonders verlässliche Zeichen einer solchen „Spur" (vgl. zum „Indiziendiskurs" Ginzburg 1995), da sie, anders als bis dato gebräuchliche individualisierende Merkmale wie Namen oder Kleider, das Risiko „der bedrohlichen Fähigkeit zur Verwandlung" (Groebner 2004: 61, vgl. Vec 2002: 5f., Cole 2002: 8ff.) der Person aufzuheben scheinen. Als nicht nur sicht- und beschreibbare, sondern vor allem in zeitlicher Hinsicht vergleichsweise konstante Merkmale verbindet sich mit der Erfassung körperlicher Merkmale im Allgemeinen und den natürlichen und künstlichen Zeichen der Haut im Besonderen die Hoffnung, wirklich einzigartige, da nur schwerlich veränderliche Zeichen und „Garant[en] der Authentizität" (Groebner 2004: 77) einer Person gefunden zu haben (vgl. Cole 2002: 12).

Angenommen wird, dass der Körper selbst etwas Erzählbares vorhält, das durch die Registrierung nicht nur zum Vorschein gebracht, sondern auch verwaltet, mithin kontrolliert werden kann. Während sich im Kontext von verschriftlichten Personenbeschreibungen Transkriptionen körperlicher Merkmale zunächst als Bestandteil einer ganzheitlichen Identifizierungsklassifikation begreifen lassen, werden Ende des 18. bzw. Anfang des 19. Jahrhunderts die körperlichen Merkmale selbst zum Gegenstand der Klassifikation. Mit dem Ziel den Körper effektiv „lesbar zu machen" (Groebner 2004: 164) entwickeln sich im Rahmen der Kriminalidentifizierung nicht nur anthropometrische Identifizierungspraktiken, wie die sogenannte Bertillonage (Cole 2002: 57f.), die durch die Erfassung spezifischer Körpermaße sowie unter Zuhilfenahme der 1839 vorgestellten Fotografie (vgl. hierzu Regener 1999) auf eine effektivere Wiedererkennung von Straftätern zielen. Vertreter populärer wissenschaftlicher Lehren, wie die Physiognomie und die Phrenologie, propagieren zudem einen mystischen Gedanken, den Groebner (2004: 86ff.) bereits in mittelalterlichen Wissenssystemen aufspürt: anhand körperlicher Merkmale auf den moralischen Charakter einer Person und insofern auf eine „innere Wahrheit" (Pugliese 2010: 25, vgl. Cole 2002: 97ff.) schließen zu können. Diese Lehren inspirieren Ende des 19. Jahrhunderts nicht nur die positivistische kriminologische Debatte um die Suche nach dem „Verbrechermenschen" (Strasser 2005, vgl. Cole 2002: 23, 57, Be-

cker 2005), in der Cesare Lombrosos 1876 erschienenes „L'uomo delinquente" vermutlich eines der bekanntesten Werke ist. Sie sind, Joseph Pugliese (2010: 25ff.) zufolge, mit ihrer Orientierung an der körperlichen Klassifizierung des ‚Anderen' zudem instrumental, den europäischen Kolonialismus zu legitimieren. Insofern legen sie auch einen Grundstein für die systematische Verwendung von Fingerabdrücken Mitte des 19. Jahrhunderts durch britische Kolonialbeamte in Indien (Cole 2002: 67, vgl. Groebner 2004: 99ff.), denn mit dem Tintenabdruck auf dem Papier, statt der bis dato gängigen verschriftlichten Personenbeschreibung, sollte eingefangen und festgehalten werden, was sich dem kolonialen Blick auf das ununterscheidbare, und mutmaßlich kriminelle, Fremde entzog:

> „Yet the civil application was in a colonial context in which the assumed inferiority of the ruled and their attendant deceptions and frauds provoked the search for greater and more efficient social control and identification." (Cole 2002: 65)

Mit dem Ziel ein handhabbares und als verlässlich eingestuftes System der Identifikation zu entwickeln, das bis zur Einführung digitaler Verfahren auf der Klassifikation und Verformelung der graphischen Merkmale des Fingerabdrucks, das heißt etwa auf Bögen, Schleifen oder Wirbeln der Papillarleisten, basierte (vgl. ausführlich dazu Meßner 2015: 243ff.), beginnt hier, wie Simon Cole (2002: 63ff.) umfänglich in seiner Geschichte des Fingerabdruckverfahrens nachzeichnet, die Umwidmung eines zunächst für zivile Zwecke genutzten Verfahrens in eine Maßnahme der kolonialen Verwaltung (vgl. dazu z.B. Sengoopta 2003) und von hier aus in eine Technologie, die, auch über die Grenzen Indiens[10] hinaus, bis heute als eines der bewährtesten Instrumente der Kriminalidentifizierung „suspekter Identitäten" (Cole 2002) gilt.

In Deutschland erfolgt die kriminalistische Identifizierung mit der daktyloskopischen Methode seit 1903 zunächst manuell, das heißt entlang einzelner Daten, die auf körperlichen Merkmalen beruhen und in Archiven bzw. Datenbanken abgelegt werden. Vor dem Hintergrund einer allgemeinen Entwicklung neuer Informations- und Kommunikationstechnologien (vgl. hierzu Gates 2005) ist 1993 in Deutschland mit dem Automatisierten Fingerabdruck-Identifizierungs-System (AFIS) im Rahmen der kriminalpolizeilichen Arbeit zudem ein automatisiertes Verfahren des Fingerabdruckvergleichs eingeführt worden. Der polizeiliche Vergleich von Merkmalen der Papillarlinien, das heißt der Beschaffenheit oder Anordnung der Grate und Furchen auf dem Fingerabdruck (zum Beispiel Überkreuzungen, Gabelungen oder das Ende von Graten), erfolgt mittlerweile in zunehmenden Maße durch Algorithmen unterstützt und neben der automatisierten Erfassung von Fingerabdruckblättern ist zudem seit

[10] Allerdings sind gegenwärtig wohl in keinem anderen Land vergleichbare Ansätze einer biometrischen Vollerfassung einer ganzen Bevölkerung wie in Indien zu beobachten (vgl. hierzu z.B. Sarkar 2014)

2006 mit dem sogenannten Fast-ID-Verfahren der Abgleich der AFIS-Datenbank mittels mobiler Fingerabdruckscanner möglich.

Fingerabdruckverfahren, als eine spezifische biometrische Technologie, lassen sich als Techniken der Vergewisserung charakterisieren, deren Anwendung – sei sie zum Zwecke der Identifizierung oder der Verifizierung von Identität – als Kernversprechen die Einzigartigkeit und Unveränderlichkeit des menschlichen Fingerabdruckes als zentrale Anwendungsprämissen zugrunde liegen (vgl. ausführlich Cole 2002, 2005). Außerhalb kriminalistischer Anwendungen blieben digitale Fingerabdrucktechnologien in Deutschland, anders als etwa in den USA (vgl. Lyon 2001: 297ff.), lange Zeit eine „Nischentechnologie", die noch in den frühen 1990er Jahren etwa nur für die Zutrittskontrolle zu Hochsicherheitsbereichen oder zur Kontrolle von Handlungsberechtigungen im Rahmen des E-Commerce eingesetzt wurde (Petermann/Sauter 2002: 61ff.). Ihre Leistungsfähigkeit galt zudem noch um die Jahrtausendwende als „nicht seriös einschätzbar" (ebd.: 99ff.) – so das Ergebnis einer Studie des Büros für Technikfolgenabschätzung des Deutschen Bundestages im Auftrag des Deutschen Bundestages. Mit diesem Gutachten sollten die „möglichen Beiträge biometrischer Verfahren zur Verbesserung der öffentlichen Sicherheit" (BT-Drs. 14/10005: 3) eruiert werden, die im Kontext der politischen Reaktionen auf die Anschläge am 11. September 2001 in New York und Washington nicht nur, aber als wesentlicher Bestandteil einer Neuen Sicherheitsarchitektur avisiert wurden. In Deutschland haben diese Reaktionen in den Folgejahren zu tiefgreifenden sicherheitspolitischen Umbaumaßnahmen geführt (vgl. Lange 2008, Glaeßner 2010) und mündeten unter anderem darin, dass Fingerabdrücke seit 2007 obligatorischer Bestandteil des neuen ePasses sind, denen im November 2010, auf freiwilliger Basis, die Fingerabdrücke im Personalausweis folgten. Seit September 2011 sind digitale Fingerabdrücke zudem im neuen elektronischen Aufenthaltstitel für Migranten verpflichtend.

Die Verbreitung biometrischer Technologien wie des Fingerabdruckverfahrens fügt sich vor diesem Hintergrund in Prozesse ein, wie sie mit dem Begriff der Versicherheitlichung oder der Securitization (vgl. Muller 2011) umschrieben werden. Dieser bezieht sich auf das Adressieren von Sicherheitsnotwendigkeiten über Unsicherheitsdiskurse: sei es durch die Praktiken von Sicherheitsexperten, „(competing for budgets and missions) and the transformation of technologies they use (computized databanks, profiling and morphing)" (Bigo 2002: 64), und den in diesem sozialen Feld bereits entwickelten Routinen und Technologien, um potenzielle künftige Gefahren zu bearbeiten, oder auch durch Sprechakte dieser Akteure, mit denen sie soziale Phänomene, erstens, als existentielle (Un-)Sicherheiten konstruieren, um diese, zweitens, mit außergewöhnlichen Maßnahmen zu bearbeiten (vgl. ebd., Buzan et al. 1998, Huys-

mans 2006). So forderte der damalige Innenminister Otto Schily bereits im Oktober 2001 in einer Rede vor dem Deutschen Bundestag den Schutz vor „unsicheren Identitäten“ durch technisch fortgeschrittene Aufklärungsmaßnahmen, wie sie die Datenvernetzung oder auch die Integration von Fingerabdrücken in Ausweispapieren als Sicherheitsmaßnahme garantieren würden (Schily 2001). Mit Fingerabdruckdaten ausgestattete Ausweisdokumente seien die Lösung „Bewegungen von Terroristen zu verhindern“ (BT-Drs. 920/01: 113) und ihr Grundstein wurde durch das am 09.01.2002 in Kraft getretene Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz, BR-Drs. 920/1/01) gelegt, mit dem Ziel, eine „Verbesserung der öffentlichen Sicherheit“ (ebd.: 25) durch eine „zweifelsfreie Identifizierung“ (ebd.) von Personen zu erreichen.

Dass Biometrie zu Beginn des neuen Jahrtausends in Deutschland als geeignete und verhältnismäßige Technik angesehen und politisch durchsetzungsfähig wurde – so verbietet das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 (BVerfGE 65: 1) ausdrücklich die Verwendung einheitlicher Personenkennzeichen und als solches gilt der Fingerabdruck aufgrund der ihm zugeschriebenen Merkmale der Eindeutigkeit und Unveränderlichkeit –, lässt sich dabei auf eine im politischen wie auch im medialen Diskurs etablierte und über globale Mobilität hergestellte Verbindung von internationalem Terrorismus, Organisierter Kriminalität und unkontrollierter Migration zurückführen (Kühne/Schlepper 2018, Klein 2011). Angesichts dieser diskursiven Verknüpfung unterschiedlicher Phänomene spricht Katja Franko Aas (2011) dann auch von einer „crimmigration“, deren Grundlagen auf EU-Ebene bereits mit dem im Jahr 2000 vom Rat der Europäischen Union umgesetzten European Dactylographic System (EURODAC) gelegt wurde. Mit EURODAC ist eine Datenbank geschaffen worden, in der die Fingerabdrücke aller Asylwerber über 14 Jahren aufgenommen und in einer zentralen Datenbank gespeichert werden (vgl. hierzu z.B. van der Ploeg 1999b). Auch das Visainformationssystem geht auf eine Entscheidung des Europäischen Rats aus dem Juni 2003 zurück und ist Teil eines sogenannten „coherent EU approach on biometrics“ (vgl. European Council 2003: 3) um „Visa-Shopping“ und „Identitätsdiebstahl“ (vgl. European Commission 2005a) zu verhindern. Biometrische Verfahren, die Unsicherheiten in Bezug auf die Authentizität von Identität durch die Verbindung von realem Individuum und seinen als unverwechselbar geltenden digital verfügbaren Körperdaten reduzieren sollen, gelten auch deshalb als „globale Kontrolltechnologie“ (Petermann 2010), weil spätestens die politischen Reaktionen auf die Anschläge am 11. September 2001 in New York und Washington verdeutlichten, dass sie zum „technologischen Herzstück“ (ebd.: 129) internationaler Grenzkontrollpolitiken geworden sind. Im Rahmen der innereuropäischen behördlichen Zusammenarbeit

wurden zum Beispiel neue Möglichkeiten der Datenerhebung und Systematisierung von Daten geschaffen: infolge des sogenannten Zugriffsbeschluss des Europäischen Rates von 2008 haben Polizei- und Strafverfolgungsbehörden sowie Geheimdienste zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer oder sonstiger schwerwiegender Straftaten auch Zugang zu EURODAC, einer der mittlerweile größten biometrischen Datenbank. Laut dem ehemaligen Bundesdatenschutzbeauftragten Schaar (2011) wurde etwa für die EU mit 20 Millionen Visaantragstellern jährlich gerechnet, die im VISA-Informationssystem erfasst werden. Vor dem Hintergrund einer solcherart zunehmenden „Versicherheitlichung von Identität“ (vgl. Muller 2004, Aas 2006, van der Ploeg 1999b) schreibt sich mit dem Einsatz der Biometrie im Rahmen nationaler Grenzregime für ihre Kritiker dann auch die Geschichte der biometrischen Identifizierung als einer Technologie, die auf Engste verbunden ist mit spezifischen Wissensregimen, fort (vgl. z.B. Muller 2011, 2004, Ceyhan 2008, Aas 2011, 2006):

> „While the imperative to identify criminal suspects and recidivists was aimed at securing the well-being of law-abiding citizens, the technologies developed for criminal identification overlapped with systematic efforts to identify and distinguish between citizens and non-citizens, determining who was entitled to the security of belonging to the nation state. […] The problem of identification and ongoing effort to improve upon and standardize identification techniques persisted throughout the twentieth century.“ (Gates 2006: 422)

Die Verbreitung biometrischer Systeme in Deutschland lässt sich zugleich als Bestandteil einer politischen Ökonomie von Technologieversprechen rekonstruieren, in der Deutschland eine Vorreiterrolle in der EU zugeschrieben wurde (Aus 2006: 17f.). In anderen Worten kann ihr zunehmend umfassenderer Einsatz nicht nur als das Ergebnis einer erfolgreichen Artikulation ‚neuer Bedrohungen‘, mit denen ein kausales Verhältnis der Technologie zu den Anschlägen vom 11. September 2001 etabliert wurde, zurückgeführt werden. Er lässt sich auch als Resultat der Bestrebungen von an politischen Prozessen beteiligten Sicherheitsexperten und ihrer Interessen beschreiben (zu den Konstruktionsprozessen der Technologie vgl. Kühne/Schlepper 2018, Kühne/Wehrheim 2013)[11]. So bildeten die politischen und medialen Deutungen des 11. September 2001 auch einen ‚großen Moment‘ des (deutschen) Biometriemarktes, der europäischen Kontroll- sowie Wirtschaftsinteressen einer neuen High-Tech-Branche Geltung verschaffte: „Sept. 11 created a long-awaited moment for the biometrics industry“ konstatierte etwa die New York Times am 17. Dezember 2001 und zitierte den Chef eines führenden Biometrie-Unternehmens: „We’ve always said that some event would have to hap-

[11] Lyon und Bennett (2008: 4ff.) sprechen im Zusammenhang mit der zunehmenden Bedeutung von Ausweisen auch von einem „card cartell“, in dem sowohl die Interessen staatlicher Behörden, privater Unternehmen und formulierte technische Standards für einzelne Verfahren zusammentreffen.

pen to propel the technology to the forefront.“ Den Forderungen der USA nach biometrischen Merkmalen in Reisedokumenten 2007 mit dem ePass nachzukommen, wie es auf europäischer Ebene durch die Verordnung 2252 vom 13. Dezember 2004 für alle europäischen Mitgliedsstaaten beschlossen wurde, bedeutete auch, eigene Überlegungen (zum Beispiel durch die Bundesdruckerei) zu einem effizienten Personenidentifikationsprozedere zu realisieren (Petermann/Sauter 2002: 54 mit Bezug auf Landvogt 2000). Auch die von staatlicher Seite erhöhte Forschungsförderung für das ‚Projekt biometrische Ausweisdokumente‘[12] baute auf Pilotprojekten auf, mit denen der Markt für kommerzielle Biometrieprodukte für breite und verlässliche Alltagsanwendungen bereits kurz vor der Jahrtausendwende geöffnet werden sollte (vgl. dazu Kühne/Schlepper 2018). An die Definition von Biometrie als Sicherheits- und Kontrolltechnologie in Bezug auf globale Mobilität und einer Neubewertung der „Sicherheit in allen Lebensbereichen“ (Petermann/Sauter 2002: 98) knüpften sich Erwartungen an einen Diffusionseffekt, Biometrie auch als eine vor allem praktische Technologie in Alltagsanwendungen einzusetzen, wie es das Joint Research Center der Europäischen Kommission 2005 formulierte: „that once the public becomes accustomed to using biometrics at the borders, their use in commercial applications will follow.“ (European Commission 2005b: 10) Und weiter heißt es im selben Papier:

> „The large-scale introduction of biometric passports in Europe provides Member States with the unique opportunity to ensure that these have a positive impact, and that they enable the creation of a vibrant European industry sector.“ (ebd.)

In den ePass wurde in Deutschland die Hoffnung gesetzt, als „Innovationsmotor für die deutsche Sicherheitsbranche“ zu wirken, so etwa der it-Lobbyverband Bitkom e.V. 2005, und dadurch auch Marktsegmente für private Anwender zu erschließen. Durch den Masseneinsatz sollte der Staat nicht mehr Hauptkunde der Biometriebranche sein, sondern die Nachfrage auch auf die Privatwirtschaft ausgedehnt werden (Bitkom 2007: 81). Bewegte sich der Umsatz des deutschen Biometriemarktes Ende der 1990er Jahre bis zur Einführung des elektronischen Reisepasses noch auf niedrigem Niveau (ebd.), erwartete Bitkom (ebd.: 82) bereits im selben Jahr auf Basis einer Studie von Global Industry Analysts für Deutschland ein Wachstum des Biometriemarktes von 100 Millionen Euro im Jahr 2005 auf 300 Millionen für 2010,

[12] Den Auftakt bildete 1999 eine gemeinsam mit dem Bundeskriminalamt (BKA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführte „Vergleichende Untersuchung biometrischer Identifikationssysteme – BioIS“. Im selben Jahr startete auch das mit 2,5 Millionen Euro durch das Bundesministerium für Wirtschaft und Technologie (BMWi) geförderte Projekt „BioTrust“. Zu diesen Projekten gehören auch die vom BSI gemeinsam mit dem BKA initiierte „Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen zum geplanten Einsatz in Lichtbilddokumenten“ „BioP I“ (11/2002-12/2003) und „BioP II“ (11/2003-12/2004), sowie die Projekte „BioFinger“ (12/2002-5/2004) und „BioFace I und II“ (2003) (BSI 2003)

und die Biometric Group ging für 2014 sogar von weltweit 9,4 Mrd. Euro jährlich aus (Bitkom 2009a). Der Nutzen lag für Akteure wie Bitkom klar auf der Hand: „Ausweise oder Passwörter können gestohlen, gefälscht, vergessen oder mutwillig weitergegeben werden – biometrische Merkmale wie Fingerabdruck, Iris, Gesicht oder Stimme hingegen sind untrennbar mit der Person verbunden." (ebd. 2007: 80)

Mittlerweile ist Biometrie als ein Sicherheitskonsumgut (vgl. Goold 2010) des Direktmarketings im Alltag angekommen, denn folgt man den Versprechen ihrer Anbieter lassen sich gegenwärtig der Einkauf im Supermarkt oder, was für das Büro für Technikfolgenforschung im Jahr 2002 noch „etwas bizarr" (Petermann/Sauter 2002: 65) klang, das Mittagessen in der Schulmensa „schnell" und „bequem" mit dem Fingerabdruck bezahlen (vgl. Böger 2012).[13]

1.1.2 Der Diskurs über Biometrie

In Diskursen über (neue) Technologien werden, zum einen, Legitimationskriterien (etwa im Sinne einer erfolgreichen Versicherheitlichung, vgl. oben) vermittelt, wie sie etwa die verpflichtende Einführung der Fingerabdruckdaten in den Reisepass begründeten. Hier werden mit Blick auf die Vor- und Nachteile der Technologie, zum anderen, die Akzeptabilitätskriterien verhandelt, die, in anderen Worten, die ‚harten Fakten' schaffen, an denen die Nutzung der Biometrie, mithin ihre Akzeptanz gemessen wird (zum Verhältnis von Akzeptanz und Akzeptabilität in der Forschung vgl. Kapitel 1.2.2ff.). Kontroversen über neue Technologien, oder in diesem Fall Auseinandersetzungen um ihren Einsatz in neuen Anwendungsfeldern, sind gleichwohl nicht untypisch. Sie machen darauf aufmerksam, dass die Bedeutung von Technologie resp. das Wissen über sie immer auch hergestellt wird, denn wie etwa Wiebe Bjiker und John Law (1992: 3) konkretisieren: Technologien „do not […] evolve under the impetus of some necessary inner technological or scientific logic. They are not possesed of an inherent momentum. If they evolve or change, it is because they have been pressed into that shape."

[13] Für eine Übersicht biometrischer Referenzprojekte (Stand 2009, vgl. Bitkom 2009b). Zur Analyse von Darstellungsweisen der Fingerabdrucktechnologie in Werbematerialien kommerzieller Anbieter (vgl. Böger 2012).

1.1.2.1 Biometrie als Sicherheitstechnologie[14]

Die Erfassung und Speicherung biometrischer Merkmale gilt in Deutschland als Lösung für eine sichere und zudem einfache Identifizierung ungewisser Identitäten, und dies auch unabhängig ihrer konkreten Anwendung wie Untersuchungen zu den sich an die Technologien knüpfenden Versprechungen im medialen wie auch politischen Diskurs nahelegen (vgl. Klein 2011, Kühne/Schlepper 2018). Bis 2007 wird die Biometrie im politischen Diskurs nahezu exklusiv als Sicherheitstechnologie im Kontext der Terrorismusbekämpfung verhandelt. Im Zusammenhang mit ihrer behördlichen Verwendung zielt die Hauptargumentation ihrer Befürworter auf die Notwendigkeit im Rahmen der Terrorismusbekämpfung mittels biometrischer Daten Strafverfolgung und Grenzkontrolle zu effektivieren (Klein 2011: 88ff.). Konkret soll mit der Integration weiterer biometrischer Merkmale aber nicht nur die „Identitätssicherung zwischen Passinhaber und Pass" (BT-Protokoll 14/209: 20754) verbessert, sondern mit dem Fingerabdruck als individuellem Merkmal die „Bindung des Ausweisdokuments an den Passinhaber" (BT-Protokoll 16/79: 7953) gestärkt werden. In diesem Zusammenhang argumentieren die Befürworter biometrischer ePässe ebenso mit der „Erhöhung der Fälschungssicherheit" (BT-Protokoll 14/192: 18702, vgl. auch BT-Protokoll 16/79: 7953) wie dem Schutz vor Identitätsdiebstahl durch verloren gegangene Ausweisdokumente (BT-Protokoll 15/129: 11844) – Szenarien, denen durch die Speicherung der Fingerabdruckdaten auf einem RFID-Chip in den Dokumenten vorgebeugt werden soll (BT-Protokoll 16/79: 7956ff.). Dabei handelt es sich um ein Argument, das mit dem Verweis auf die Sicherheit der bisherigen Ausweisdokumente gleichwohl Zweifel an der Legitimität des Sicherheitsversprechens hervorgerufen hat. Wie die Antwort der Bundesregierung auf eine Kleine Anfrage der Linken ergab (vgl. BT-Drs. 16/5507: 1f.), waren etwa im Zeitraum von 2001 bis 2006 lediglich sechs Totalfälschungen und 344 Verfälschungen von deutschen Pässen zu verzeichnen, die zudem in keinem Zusammenhang zu terroristischen Anschlägen standen. Ungeachtet dessen wurde mit neuen staatlichen Forschungsförderungen das ‚Projekt biometrische Ausweise' weiter vorangetrieben (Kühne/Schlepper 2018).[15]

Allerdings verliert das Sicherheitsargument mit dem Beginn der Debatte um ihre freiwillige Aufnahme in den Personalausweis zunehmend seine klaren Konturen. Dies zeigt sich, zum einen, in einer zunehmenden „crimmigration" (Aas 2011), da, wie Inga Klein (2011: 90) kon-

[14] Eingang in die nachfolgenden Darstellungen finden in überarbeiteter Form Ergebnisse einer Analyse zu den Versprechensdiskursen der Biometrie in Deutschland, die 2018 bereits an anderer Stelle veröffentlicht wurden (Kühne/Schlepper 2018).

[15] Es handelt sich dabei um die Projekte „BioP I" (11/2002-12/2003), „BioP II" (11/2003-12/2004), „BioFinger" (12/2002-5/2004), „BioFace I und II" (2003) (vgl. dazu BSI 2003).

statiert, im Rahmen des Diskurses rund um die Einführung des ePasses neben Terroristen neue Unsicherheitsargumentationen aktivierende Akteure, etwa ‚Kriminelle' und ‚illegale Einwanderer', in die Grenzziehungen zwischen ‚Freund' und ‚Feind' (ebd. 2011: 88ff., vgl. auch Kühne/Schlepper 2018) Einzug halten. Für die Bewerbung des neuen Ausweises erweist sich, anders als beim ePass, statt dem Fingerabdruck, zum anderen, vor allem die „Onlinefunktion" als Möglichkeit der Verifikation etwa im Rahmen des e-Government als zentral, mit der sich zudem Erwartungen eines großen Marktpotentials verbinden (VDI/VDE-IT 2009: 44). So soll der neue Ausweis zum Standard des Identitätsnachweises im Internet werden (BMI 2010: 10) und Praktikabilitätsargumente für weitergehende Authentifizierungen gewinnen auch im Kontext der Bewerbung des ePasses zunehmend an Bedeutung. Biometrische Merkmale im Reisepass gelten nicht nur als ein „konkreter Sicherheitsgewinn" (BT-Protokoll 16/100: 10242), sondern sie seien überdies auch praktisch, da sie zum Beispiel gleichsam die gegenwärtige Grenzkontrolle in ihren Abläufen beschleunigen würden, so etwa der Abgeordnete Hofmann in der Plenardebatte am 01.02.2007:

> „Trotz Datenschutz dürfen wir uns technischen Innovationen nicht verschließen. Durch biometrische Merkmale im Pass wird es möglich, die Identität von Personen, vor allem bei Grenzkontrollen, durch Vergleich mit den Merkmalen der kontrollierten Person festzustellen. Dies verhindert in großem Maße die missbräuchliche Nutzung und ermöglicht eine schnellere sowie exaktere Kontrolle. Mehr Sicherheit und geringere Wartezeiten an den Grenzen sind die Folge." (BT-Protokoll 16/79: 7953)

Auch der Informationsfilm des Bundesministeriums des Inneren (2007) zum ePass illustriert, dass nicht nur die Bewegungen von Terroristen, sondern Mobilität generell zum Problem gerät und auch das Werbeplakat des BMI (Juli 2007) stellt mit dem Slogan „Der elektronische Pass – mit Sicherheit mobil" dieselbe Verbindung her. Wachse, wie dann auch das Bundesamt für Sicherheit in der Informationstechnik (o.J.a) zu den Grundlagen der biometrischen Authentisierung erklärt, der Bedarf an „zuverlässigen Personenidentifikationen" in einer „vielfach elektronisch kommunizierenden Welt mit mehr als 6 Milliarden Menschen" mittels eindeutiger Merkmale, statt Verfahren, die auf den Besitz eines Objektes setzen, dann korrespondiert diese Umdeutung bzw. Vervielfältigung der Sicherheitsversprechen mit einer doppelten Logik der Sicherheitsproduktion, in der Prävention und das Sicherheitsmanagement von Mobilität Hand in Hand gehen (vgl. Amoore 2008: 23ff.). So wird auch für das Sicherheitsversprechen konstatiert, dass in Deutschland Mobilität zur

> „Voraussetzung neuer erweiterter polizeilicher Sichtbarkeitsregime [geworden ist], deren Zweck in der Schaffung kontrollierbarer, auf ihre Echtheit, Vertrauenswürdigkeit, Zuverlässigkeit und Störungsfreiheit überprüfbarer Identitäten von Menschen und Dingen liegt, die in den Netzen der Kommunikation und des Verkehrs fließen." (Hempel et al. 2011: 14)

Ein sich in den Argumentationen der Biometrie-Befürworter abzeichnender Wandel hin zu bürgerlichen Bedürfnissen nach Komfort und Distinktion im alltäglichen Handeln in einer globalisierten Welt ist, analog zu den frühen Ansätzen einer Marketingstrategie vor 2001, deren Prämisse lautete, dass für die „Nutzer […] Biometrie mehr Komfort schaffen [kann], denn ‚man hat sich ja immer dabei'" (Büllingen/Hillebrand 2000: 339), sowohl in der Bewerbung kommerzieller Anwendungen (vgl. Böger 2012) als auch im politischen Diskurs zu identifizieren, gleichwohl nicht darauf beschränkt (vgl. hierzu Kühne/Schlepper 2018). So werden etwa auch Distinktions- oder Prestigegewinne (Albrecht 2002: 93) dort erwartet, wo eine biometrische Registrierung dazu dienen soll, Abläufe zu erleichtern: etwa im Rahmen von Vielfliegerprogrammen, wenn Biometrie die schnellere Abwicklung des Check-in ermöglicht, oder bei Stammkunden von Kneipen und Diskotheken, denen auf diese Weise nicht nur das Bezahlen oder das Eintrittsprocedere erleichtert würde, sondern die durch die Nutzung biometrischer Authentifizierung symbolische Aufwertungen erwarten dürften.

1.1.2.2 Biometrie als Risikotechnologie

Für den kritischen Diskurs sind biometrische Daten demgegenüber weniger eine Frage der Sicherheit, sondern eine des Risikos und dies nicht nur, weil ihre zunehmende Anwendung innerhalb von Grenzregimen als eine gelesen wird, mit der soziale Ordnungsvorstellungen durchgesetzt werden – so stellt auch Valentin Groebner (2004: 180) heraus, dass „in der Geschichte des Identifizierens […] die Position der Ausgeschlossenen, Nicht-Identifizierten immer präsent (ist)" –, sondern weil Identifizierungsverfahren geeignet seien, in die Identitätsbildung einzugreifen. In anderen Worten wird die Bedeutung der (bürokratischen) Bescheinigungen persönlicher, auch körperlicher Details für Praktiken der Identifizierung und Wiedererkennung nicht nur darin gesehen, dass sie zum Stellvertreter für ein (nicht-)teilhabeberechtigtes politisches Subjekt werden, dem Rechte und Pflichten zugeordnet oder vorenthalten werden können (ebd.: 162, vgl. Cole 2002: 8ff.), sie mithin über Ein- oder Ausschluss von Personengruppen entscheiden. Weil Körper-Daten zudem grundlegend für ein auf diese Weise vermitteltes authentisches Subjekt stehen (Caplan 2001: 51, Groebner 2004: 123), gewinnt ein solches „governing by identity" (Amoore 2008) vor dem Hintergrund der Entwicklung neuer Informationstechnologien eine neue Qualität, die im Bild des maschinell lesbaren Körpers (vgl. van der Ploeg 1999a) seinen Ausdruck gefunden hat: „The body [...] is treated like a text. It becomes a password, providing a document for decoding." (Lyon 2001: 299, vgl. auch Aas 2006: 144f.) So werden (idealtypisch, vgl. ausführlicher dazu Maltoni et

al. 2009) im Rahmen automatisierter Authentifizierungsprozesse körperliche Daten mittels Sensortechnik gelesen und die so erfassten Bilder mittels Algorithmen in ein sogenanntes Template[16] umgewandelt, welches als Referenzdatei Eingang in eine Datenbank findet. Zum Zwecke der Identifikation erfolgt der Abgleich der von einer Person präsentierten, ebenfalls im Prozess des ‚Lesens' umgewandelten, körperlichen Daten mit den in der Datenbank gespeicherten Templates (1:n). Für eine Verifikation der Person, also die Überprüfung, ob die Person tatsächlich die ist, die sie behauptet zu sein, erfolgt die Kontrolle analog dazu mit dem gespeicherten Referenztemplate (1:1). Weil die reale Person auf diese Weise hinter maschinenlesbaren Codes verschwindet, sind es dann Datenbanken, die die Konstruktion von Identität übernehmen: digital, über statistisch begründete Zuschreibungen und Daten (Aas 2006: 154, Lyon 2001: 306). Eine solche ‚Sprache' abstrahiere aber nicht nur von einer „persönlichen Wahrheit", wie sie in sozialer Interaktion hergestellt wird (Aas 2006: 153), sondern auch vom Körper, den „words made of flesh" (Mordini 2009: 300), selbst. Wenn biometrische Daten die Qualität einer Kommunikationstechnik erhalten, die binär codierte (ja-nein, richtig-falsch), scheinbar eindeutige Ergebnisse hervorbringt und, indem sie die „Definitionsmacht" (Feest/Blankenburg 1972) weitgehend auf technische, vermeintlich fehlerfreie, Systeme überträgt, verändert diese auch die „Beschwerdemacht" (ebd.: 19). Thematisiert werden im Risikodiskurs dann auch Erkennungsprobleme, die sich daraus ergeben, dass, etwa im Hinblick auf biometrische Verfahren die zum Beispiel Zugang gewährleisten sollen, das Funktionieren der Technologie grundsätzlich abhängig ist von definierten Toleranzwerten, die sich entlang von Falschakzeptanzraten (FAR) und Falschrückweisungsraten (FRR) wechselseitig verändern: das heißt je niedriger die FAR, desto höher die FRR und umgekehrt (Hornung 2007: 142, Kurz 2008: 107). Risiken ergeben sich also auch entlang der sogenannten „biometrischen Performanz" (Bromba 2007: 194), wenn etwa körperliche Merkmale bestimmter Bevölkerungsgruppen nicht erfasst werden können (vgl. Kurz 2008: 106ff.). Eher selten wird in diesem Zusammenhang darauf aufmerksam gemacht, dass die biometrische Performanz gleichsam an kulturelle Verständnisse wie zum Beispiel Alter, Gender oder Rasse gebunden ist. Joseph Pugliese (2010) etwa konstatiert angesichts der engen Verzahnung geopolitischer Interessen und rassifizierter Agenden, die die Entwicklung der Technologie von Beginn an begleiten, eine „infrastructural calibration of whiteness" (ebd.: 94) für biometrische Verfahren, die ihren Ausdruck in unterschiedlichen Fehlerraten beim Einlesen von Menschen unterschiedlicher Ethnien findet (ebd.: 59, so auch Neyland 2009, Magnet 2011) und dazu führt, dass „ille-

[16] Ein Template lässt sich als eine kompakte Beschreibung eines biometrischen Musters definieren. Es stellt einen digitalen Kode dar, wenngleich auch unbearbeitete Bilder des Fingerabdrucks mitunter gespeichert werden (Ross et al. 2007: 544).

gible biometric bodies emerge around and between readable bodies.“ (Murray 2007: 350) Biometrische Technologien und ihre Funktionalität sind danach nicht nur das Ergebnis von Konstruktionsprozessen der an ihrem Werden Beteiligten (vgl. hierzu auch Meßner 2015). Auch biometrische Daten selbst, und darauf weist eindrücklich vor allem Simon Cole (2002, 2005, 2008) hin, mussten und müssen immer auch interpretiert werden und unterliegen somit Prozessen sozialer Be-Deutung. Biometrische Daten als Informationen werden „collected, sorted, and sent, literally, by the work of people“ (Walby 2005: 161). So ist die Identifikation entlang von Fingerabdruckmerkmalen eine Suche nach Übereinstimmungen bereits vorab definierter Merkmale bzw. Merkmalskategorien (Cole 2008: 109), für deren Bestätigung sich etwa allein im Rahmen der Kriminalidentifizierung in unterschiedlichen Ländern gegenwärtig nicht nur variierende Grenzwerte dafür ausmachen lassen, ab wie vielen Übereinstimmungen von Minutien zwei Fingerabdrücke als identisch gelten.[17] Es variieren auch die Bestimmungen dafür, welche Merkmale der Fingers überhaupt zur Identifizierung herangezogen sollten.[18] Im 6. Kapitel des Fingerprint Sourcebook beschreiben Moses et al. (2011: 6–24) die Einschreibung der interpretativen Vorleistung, oder in den Worten Coles (2008: 119) die „opinionization“ des Fingerabdruckvergleichs in die Automatisierung, ebenso anschaulich wie schlicht als technisierten Imitationsprozess: „Automatic fingerprint feature-extraction algorithms were developed to imitate minutiae location performed by forensic experts.“

Wenn in dieser Hinsicht Bestimmungen der Leistungsfähigkeit der Technologie relevant werden, sind damit auch Konstruktionsprozesse der Technologie selbst angesprochen, die vor allem mit Blick in ihre historische Konstitution identifiziert werden, im medialen und/oder politischen Diskurs um die Bedeutung der Technologie gleichwohl eine eher geringe Relevanz entfalten. Obwohl die Konstruktion von Sicherheit im Medium einer Technologie erfolgt, die auf bestimmten Formen des Wissens beruht, welche spezifische Gegenstands- und Interventionsfelder produziert (Krasmann et al. 2014: 14), wird im medialen Diskurs weder das konstruktive Moment der Technologie (vgl. Krasmann/Kühne 2014) thematisch, noch Fragen von Exklusion, die den Einsatz der Biometrie historisch begleiten und im Rahmen von gegenwärtigen Grenzregimen ihre Aktualisierung erfahren. Dies konstatiert Inga Klein (2011) dann auch für den eher kritischen medialen und bürgerrechtlichen Diskurs. Biometrie, so Klein (ebd.: 91f.), erscheine aufgrund einer tendenziell einseitigen Historisierung als die „Technik der ‚Guten‘“. Symbolisieren einer Studie von Prainsack und Kitzberger (2009) zu-

[17] In Deutschland liegt dieser Wert bei zwölf Minutien (BSI o.J.b: 10). In Großbritannien etwa gilt seit 2005 ein Minimum von acht übereinstimmenden Minutien für die Identifizierung. In Italien und Frankreich hingegen sind es 16 und in Brasilien und Argentinien sogar 30 (Meintjes-Van der Walt 2006: 166).

[18] Eine ausführliche Geschichte der Individualisierungsprotokolle, das heißt zu den Vorschriften zum Ablauf des Vergleiches und der Entscheidungsdefinitionen in Großbritannien und den USA findet sich bei Cole (2002).

folge Fingerabdrücke zudem als traditionelles Merkmal der Individualisierung bis heute typischerweise den strafrechtlichen Zugriff des Staates auf seine Bürger, entfaltet sich ein Element einer bürgerrechtlichen Kritik an der Verbreitung der Technologie auch eher daran, dass mit der Integration von Fingerabdrücken in Ausweisdokumente Stigmatisierungs- und Degradierungseffekte einhergehen, weil die etablierte juridische Grenzziehung, die die Technologie im polizeilichen Anwendungsbereich kennzeichnet, unterlaufen werde:

> „Mit §81b StPO wurde eine Ermächtigungsgrundlage für erkennungsdienstliche Maßnahmen geschaffen. Diese erkennungsdienstlichen Maßnahmen waren bislang nur gegenüber Beschuldigten einer Straftat zulässig. [...] Wer gezwungen ist, seine Fingerabdrücke bei einer Behörde zu hinterlegen, fühlt sich als Verbrecher behandelt." (Selbmann 2008: 31, vgl. ähnlich auch Kurz 2008: 104, Lyon 2001: 300f.)

Als eine „Misstrauenserklärung" an die Bevölkerung fasst dann auch Rolf Gössner (2002) die Integration von digitalen biometrischen Daten in nationale Identitätsdokumente, denn die Bürger müssen sich nun „behandeln lassen wie bislang nur Tatverdächtige oder Kriminelle im Zuge einer Erkennungsdienstlichen Behandlung". Oliver Lepsius (2004: 78ff.) spricht in diesem Zusammenhang auch von einer „Entindividualisierung im Sicherheitsrecht". Als mittlerweile etablierter Teil von deutschen Identitätsdokumenten erscheinen die biometrischen Daten als Bestandteil eines „visible imperative" (Haggerty 2009: 161), der ein fehlendes Vertrauen des Staates in (die Freiheit) seine(r) Bürger bekundet (vgl. Goold 2009). Der Bürger wird gleichsam sichtbarer, während die Kontrolltechnologien selbst unsichtbar: kleiner, mobiler, unscheinbarer werden (Murakami-Wood 2011).

Befürchtet werden mit dem Einsatz der Technologie dann auch Risiken für die Privatheit. Wenn der Körper selbst mittels Algorithmisierung Eingang in digitale Informationskontexte findet, dann, so etwa Irma van der Ploeg (2003a, 2003b), lässt sich die Bedrohung dieser nicht allein im Konzept der informationellen Privatheit, das heißt einer Kontrolle darüber, wann und in welchem Ausmaß persönliche gespeicherte Daten anderen verfügbar gemacht werden (vgl. auch Rössler 2001: 25), auflösen. Vielmehr ist sie dann explizit mit dem Begriff der körperlichen Privatheit verbunden. Da es nicht nur darum gehe, ob Eingriffe in die körperliche Integrität von Personen zulässig sind, sondern auch wie Körpereigenschaften digital repräsentiert werden, plädiert van der Ploeg (2003b) deshalb auch dafür, dass die Preisgabe körperlicher Daten selbst strengeren Datenschutzregulierungen unterworfen werden sollte (vgl. mit vergleichbaren Anmerkungen auch Petermann/Sauter 2002: 90). Sie argumentiert, dass „bodily integrity applies to the ‚thing itself', whereas informational privacy is presumed

to cover all (digital) ‚representations' of it." (ebd.: 67)[19] Die Referenz der Kritik bildet insofern ein Begriff von Privatheit, der sich, wie die informationelle Selbstbestimmung, als Kontrolle gegenüber den Einsprüchen und Eingriffen Dritter behauptet, seine Erweiterung aber darin findet, auch Autor der eigenen Identität bleiben zu können. Obzwar biometrische Daten als personenbezogene und mithin private Daten gelten (vgl. Rössler 2001: 221f.) wird allerdings in der Regel ein dem Eigentum vergleichbares Recht an persönlichen Daten nicht nur verneint (vgl. dazu Nettesheim 2000: 27). Im Hinblick auf die eindeutige Bestimmbarkeit mittels körperlicher Daten wird angesichts von Anonymisierungsmöglichkeiten durch Algorithmen sogar eine Relativität des Personenbezugs diskutiert (vgl. z.B. Hornung 2005: 142ff.)[20]. Unzumutbarkeiten biometrischer Technologien im Hinblick auf die Bewahrung der körperlichen Integrität erscheinen vielmehr im Risiko der Bemächtigung einer Identität qua Körpermerkmal, wenn etwa gewalttätige Zugriffe wie Entführungen, Erpressungen und sogar das Abtrennen der Finger von Merkmalsträgern befürchtet werden (vgl. Kurz 2008: 112).

Als ein zentrales Moment des Risikodiskurses erweist sich insofern die Möglichkeit des Zugriffs auf die biometrischen Daten, die das im Volkszählungsurteil vom Bundesverfassungsgericht umrissene Recht auf informationelle Selbstbestimmung deshalb gefährdet, weil die unautorisierte Verwendung der preisgegebenen Daten wahrscheinlich erscheint und die Möglichkeit, den Zugang von Dritten auf persönlichkeitsrelevante Informationen restringieren zu können – die sogenannte „informationelle Privatheit" (Rössler 2001: 25) – angezweifelt wird. Bezweifelt wird in diesem Zusammenhang dann auch die Funktionalität biometrischer Systeme. Befürchtet werden neue „Begehrlichkeiten" (Kurz 2008: 108) und mit der Einführung der neuen Ausweisdokumente die „biometrische Vollerfassung" (ebd.), weil etwa auch die technische Verlässlichkeit der Speichermedien, etwa des RFID-Chips in den Ausweispapieren, in Frage gestellt wird. Denn obwohl das Passgesetz vom 24. Mai 2007 und das Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 18. Juni 2009 eine zentrale Speicherung der Fingerabdruckdaten ausdrücklich untersagen, böten insbesondere kontaktlos auslesbare RFID-Chips als neues Speichermedium fast unbegrenzte Möglichkeiten für eine unautorisierte Nutzung der biometrischen Daten (Kurz 2008: 108f., Eisenberg et al. 2005: 93, Murakami Wood et al. 2006: 24ff., Hornung 2005, 2007). Wird der Fingerabdruck in der medialen und politischen Deutung, auf der einen Seite, als eine die Privatheit des Bürgers sichernde Technologie präsentiert – das persönliche Merkmal ist gesichert durch Digitalisie-

[19] In diesem Sinne argumentiert auch Saborowski (2008: 85), wonach aus dem Körper gewonnene Daten nicht einfach als „verfügbare ‚Sache'" zu behandeln seien.

[20] So wird der Personenbezug in Abhängigkeit von der Verarbeitungsphase, in der die Daten Anwendung finden, ihrer Erscheinungsform und der jeweiligen Datenspeicherung bewertet (vgl. Hornung 2004: 429ff., Petermann/Sauter 2002: 87).

rung und Verschlüsselung und in diesem Sinn, ‚versteckt' im RFID-Chip –, lautet das Gegenargument, dass RFID-Chips immer mehr Personen und Institutionen zugänglich würden und so unbefugt sowie unbemerkt ausgelesen werden könnten (Hornung 2005, 2007, Murakami Wood et al. 2006: 24ff.). Auch dem Argument, biometrische Verfahren seien geeignet Zugriffssicherung auf personenbezogene Daten zu ermöglichen, indem sie deren Zugänglichkeit individualisieren und personalisieren (Probst 2002: 125, Bäumler et al. 2001: 20ff.), mithin sichern, wird so regelmäßig das Risiko des Identitätsdiebstahls gegenübergestellt, das sich gerade durch den Einsatz der als individuell klassifizierten Merkmale realisieren könnte (Pfitzmann 2005: 155, Kurz 2008: 110). Dass hierfür die Daten nicht einmal ‚ausgelesen' werden müssen, demonstrierte der Chaos Computer Club (CCC) 2008 durch die ‚Entführung' des Fingerabdrucks Wolfgang Schäubles, den dieser auf einem Wasserglas hinterlassen habe und dessen Kopie der Club in seiner Mitgliederzeitung „Die Datenschleuder" veröffentlichte (CCC 2008: 56f.).

Der Fingerabdruck, so die Kritik an solcherart Sicherheitslücken der Technologie, lasse sich aber nicht nur problemlos vervielfältigen, sondern auch verteilen. Befürchtet wird dann auch eine Flexibilisierung und Dekontextualisierung biometrischer Daten (Kurz 2008: 108f.), die sich durch die Vernetzung mit verschiedenen, in unterschiedlichen Kontexten erhobenen, Daten ergeben. Sowohl innerhalb des medial verfügbaren bürgerrechtlichen, als auch des akademischen Diskurses wird befürchtet, dass das, was technisch möglich sei, auch realisiert, mitunter sogar nachträglich legalisiert werden könne (vgl. Eisenberg et al. 2005: 93, Strasser 2006: 24f.). Entsprechende Entwicklungen unterstützen diesen Argwohn: Die geplante Aufhebung der Zweckbindung der EURODAC-Datenbank etwa, die ursprünglich angelegt wurde, um das sogenannte ‚visa shopping' (European Commission 2005: 4) zu verhindern und auf die zukünftig auch europäische Strafverfolgungsbehörden Zugriff erhalten sollen, lässt auch den Zugriff auf die im Reisepass gespeicherten Daten befürchten (Prantl 2012). Der Datenmissbrauch bildet den zentralen Gegenentwurf zum Sicherheitsversprechen, weil die potentielle Bildung detaillierter Persönlichkeitsprofile und eine typisierend-automatisierte Einordnung des Einzelnen anhand abstrakter Kriterien das Risiko in sich trage, die Informationen über die eigene Person nicht mehr selbsttägig kontrollieren zu können. Befürchtet werden dann auch sogenannte Überschussdaten, die sich aus den biometrischen Daten ableiten ließen. Andreas Pfitzmann (2005: 156) etwa verweist in diesem Zusammenhang auf Untersuchungen, die der Frage nachgehen, ob sich anhand von Fingerabdrücken auf die sexuelle Orientierung einer Person schließen lasse.

Als ein weiterer zentraler Begriff innerhalb der Szenarien des potentiellen „function creep“ (Mordini 2009: 294ff.), das heißt der erweiterten Verwendung der Daten, erweist sich jener der Data Doubles (Haggerty/Ericson 2000: 606) – sogenannter virtueller Doppelgänger auf Basis des Templates innerhalb von Datenstrukturen der „surveillance assemblage“ (ebd.). Mit ihnen ließen sich nicht nur Informationen über reale Personen vereinigen, die auf die Vergangenheit verweisen – bei Zugangsverfahren etwa der Zeitpunkt des Betretens des Gebäudes. Wenn biometrische Verfahren in dieser Argumentation primär als technologisches Moment des Risikomanagements fungieren (Lyon 2001: 303), ihr Einsatz, in anderen Worten, orientiert ist an dem proaktiven Einhegen zukünftiger Risiken, dann könnte, so etwa David Lyon (ebd.: 307, hier mit Bezug auf die Potentiale der Gentechnologie), „the next stage“ (ebd.), darin bestehen, dass, indem der Mensch über die so verfügbar werdenden Datenzuhänge kategorisier- und kalkulierbar werde, auch in die Wahlmöglichkeiten seines Handelns eingegriffen werden könne.

Treten im Risikodiskurs die Akteure der Kontrolle in den Vordergrund (vgl. z.B. Lyon 2001), denen mit dem digitalen Fingerabdruckverfahren Möglichkeiten einer neuen Qualität von Missbrauch und Kontrolle an die Hand gegeben werden, dann ist die Verhandlung der Technologie auch eingebettet in einen größeren Überwachungsdiskurs. Wie Inga Klein (2011) für den politischen und medialen Diskurs und auch eine eigene Analyse nachzeichnen (Krasmann/Kühne 2014)[21] konnte, erfahren die mit der Technologie verknüpften Risikoszenarien vor allem in Schlagworten wie dem „gläsernen Menschen“, „George Orwell“ oder „Big Brother“ ihre Konkretisierung. Inga Klein (2011) identifiziert im Diskurs um die Einführung des ePasses dann auch eine doppelte Subjektpositionierung: auf der einen Seite die sich vervielfältigenden ‚gefährlichen‘ Subjekte und ihnen gegenüber die ‚Bürger‘, an die sich – über die Adressierung diverser Gefährdungslagen, zum Beispiel Terrorismus, der Diebstahl der Papiere oder Betrugsversuche – das Sicherheitsversprechen richtet. Weil (politische) Sicherheitsdiskurse eine Steuerungsfunktion entfalten (vgl. Zurawski 2007: 10), sie Teil des Unsicherheitsmanagements sind, wird dann auch befürchtet, dass das Thematisieren von realen oder nicht realen Unsicherheiten für die Bürger eine handlungsleitende Funktion entfalten könne (vgl. O‘Malley 2004: 15). Einen solchen Zusammenhang vermutet etwa Aldo Legnaro (2011: 196) für die Akzeptanz der biometrischen Ausweispapiere:

[21] Es handelte sich dabei um eine Inhaltsanalyse von 177 deutschen Zeitungs- und Zeitschriftenartikeln, die zwischen 2001 und 2010 erschienen und die Einführung von Fingerabdrücken in den ePass und den Personalausweis thematisieren.

> „Die biometrischen Ausweispapiere der nahen Zukunft sind zwar keineswegs kostenlos, dafür aber obligatorisch, sodass das Versprechen von Sicherheitsgewinnen genügt, um verbreitete Akzeptanz zu erzeugen."

Aus einer ursprünglich als Kriminalisierungstechnik entworfenen Technologie könne eine Maßnahme des persönlichen Schutzes werden. Weil auch im ökonomischen Kontext Sicherheit zu einem Thema wird, mit dem sich Ängste und Verantwortlichkeiten mobilisieren ließen, fürchtet dann auch der Informatiker Sachar Paulus (2011: 152), dass der Wille der Bürger neue Technologien der Sicherheit und Kontrolle zu nutzen von subjektiven Bedrohungsgefühlen geleitet und mit der Bereitschaft verbunden sei „Einschränkungen der Freiheit in Kauf zu nehmen – das ist aber gefährlich". Allerdings fungiert, auf der anderen Seite, so die Analyse Kleins (2011) auch die Fokussierung auf den Topos des Identitätsdiebstahls und/oder der daran anschließenden Überwachungsdystopien ebenfalls als Adressierung der Bürger, sich konkret als gefährdet im Hinblick auf die eigenen Sicherheitsbelange zu begreifen, welche durch die zukünftigen Risiken bedroht würden (ebd.: 90ff.). So sind die Deutungsmuster in beiden Diskurssträngen, so Klein (ebd.: 94), auf Zukünftiges gerichtet und setzen in gleichem Maße auf „Hoffnungen, Wünsche und Überzeugungen ebenso wie Ängste und Befürchtungen" und dies auch unabhängig konkreter Erfahrungen und Praktiken im Umgang mit der Technologie selbst (ebd.: 97). So sähe sich der Bürger also nicht nur immer häufiger aufgefordert, private Daten preiszugeben, sondern er steht auch in der Verantwortung, seine privaten Daten selbst zu schützen.

1.2 Über Akzeptanz

Die Rede von und über die Akzeptanz ist vergleichsweise jüngeren Ursprungs. Erst in den 1970er Jahren findet der Begriff Eingang in das Repertoire sozialwissenschaftlicher Disziplinen und – von wenigen Ausnahmen abgesehen – ab Ende der 1980er Jahre auch in soziologische Hand- und Wörterbücher (Lucke 1995: 46f.). Die gesellschaftliche Befasstheit mit Akzeptanz ist, folgt man Doris Lucke (ebd.: 140ff.), die 1995 mit ihrer Monografie die bislang umfassendste Auseinandersetzung mit dem Akzeptanzkonzept vorgelegt hat, ein modernes Projekt, denn sie ist, und dies eint zugleich die sich seither im Schnittfeld von Wirtschaftswissenschaften, Psychologie und Technikforschung entwickelte Akzeptanzforschung, von der Annahme geleitet, wonach in demokratischen Gesellschaften ein Mindestmaß an Zustimmung und Anerkennung, Annahme oder Toleranz erforderlich, gleichsam aber als zunehmend

schwer mobilisierbar scheint.[22] Akzeptanz ist, wie nachfolgend dargestellt wird, zum gesellschaftlichen Schlüsselbegriff von Gegenwartsgesellschaften geworden. Vor diesem Hintergrund hat sich eine spezifische Tradition der Akzeptanzforschung etabliert, die sich auch in der Auseinandersetzung mit der Akzeptanz von neuen Technologien der Sicherheit und Kontrolle widerspiegelt.

1.2.1 Akzeptanz als gesellschaftstheoretischer Schlüsselbegriff

Wie Doris Lucke (1995) in ihrer Habilitationsschrift entfaltet und sich entlang der zunächst vor allem techniksoziologischen Befasstheit mit dem gesellschaftlichen Unbehagen an Technik eruiert lässt, erwächst der Begriff der Akzeptanz aus der (gesellschaftlichen, politischen und wissenschaftlichen) Reflexion einer Krise seiner selbst, die auf engste verknüpft ist mit der Diskussion um Modernisierungsrisiken und damit einem „Anwachsen kausaler Komplexität, als der Vielzahl und Verschiedenartigkeit von Ursachen und Nebenwirkungen, die in das eigentlich gewollte Geschehen eingeflochten sind." (Luhmann 2003: 99) So sind es vor allem die seit dem Ende der 1960er Jahre als Problem ausgemachten Ausdrucksformen einer fehlenden Anerkennung von Technik, die den Ausgangspunkt der begrifflichen Karriere der Akzeptanz markieren. Zunehmend skeptische, zuweilen als ‚technikfeindlich' charakterisierte, Einstellungen der Bürger, wie sie etwa die Ergebnisse der Meinungsumfragen des Instituts für Demoskopie Allensbach (IfD)[23] vermitteln, geraten nicht nur zu einem medial präsenten Thema (vgl. Kistler 2005, Gloede/Hennen 2005, Petermann/Scherz 2005, Jaufmann 1999). Jenes neue Technikunbehagen findet seit den 1970er Jahren zudem seinen Ausdruck in öffentlichen Kundgaben von Kritik. Prominente Beispiele dafür sind etwa der zunächst eher „regionalistische" (Ehmke 1987: 10, vgl. auch Kliment 1994: 39f.) und später durch eine Vielzahl von etablierten und neuen sozialen Bewegungen getragene öffentliche Protest gegen die Atomkrafttechnologie (Dierkes/Marz 1993: 18) oder der sich vom Expertendiskurs (Berlinghoff 2013) zu zahlreichen Boykottinitiativen etablierende Widerstand gegen die „Gefahren der Personalinformationssysteme" und die Volkszählung (vgl. Hubert 1983).

Technologiekritik und „das Unbehagen an der Modernität" sind freilich kein Novum des 20. Jahrhunderts (Renn 1986: 48, vgl. Luhmann 2003: 135ff., Kistler 2005: 13).[24] Die Besonderheit des neuen Konfliktes um Technik, innerhalb dessen sich der Akzeptanzbegriff etabliert,

[22] Zu den Theoremen über den Modernisierungsprozess siehe Lepsius (2009: 225ff.).
[23] Zu einer Kritik an den in den Befragungen verwendeten Indikatoren siehe Jaufmann (1999).
[24] Insbesondere zur Einordnung der Technikakzeptanz als eine Frage des geschichtlichen Verhältnisses des Menschen zur Natur und Technik vgl. Oldemeyer (1988: 37ff.).

liegt darin, dass die „Idee eines zeitlich-unbegrenzten Kulturfortschritts“ (Oldemeyer 1988: 42) nun in dem Maße öffentlich kritisiert wird, wie, zum einen, technologische (Neben-)Folgen zunehmend im öffentlichen Diskurs verhandelt werden – etwa die größeren, sich keiner objektiven Risikobilanz mehr fügenden Störfälle der Atomtechnologie oder das unter dem Begriff der „Verdatung“ verhandelte potentielle informationelle Ungleichgewicht aufgrund der Einführung der Mikroelektronik in die Arbeitsprozesse der staatlichen Behörden (vgl. Berlinghoff 2013, Pethes 2004). Zum anderen werden diese Risiken lebensweltlich verfügbar. Ergibt sich die Virulenz der Akzeptanzfrage vor dem Hintergrund eines Erodierens gesellschaftlicher Erwartungssicherheiten, wird zunehmend nach einer Abschätzung von Technikfolgen, das heißt potentieller Risiken verlangt. Indem Ereignisse zunehmend im Modus des Risikos erfasst werden (vgl. Bonß 1996) eröffnet dies das Feld der Risikokommunikation über „wissenschaftsinduzierte Unsicherheiten“, die die Gesellschaft mit nicht mehr handhabbaren Folgeproblemen konfrontieren (Bonß 1995: 219ff; 1996: 178).

Die gemeinhin als technikfeindlich deklarierte Einstellung der Bürger auf den Prüfstand stellend, befördert die sich in den 1980er Jahren und 1990er Jahren etablierende akzeptanzorientierte Techniksoziologie (vgl. Gloede/Hennen 2005: 4ff.) etwa die Erkenntnis, dass sich mit einzelnen Technologien gänzlich unterschiedliche Bewertungen verbinden (vgl. Renn 2005, Jakobs et al. 2009, Grunwald 2005). Nimmt diese Forschungsrichtung ihren Ausgangspunkt an der gesellschaftlichen Beunruhigung über den fortschreitenden Technikeinsatz und die Kontroverse von Gefährdungspotentialen sogenannter Risikotechnologien, kann sie zudem zeigen, dass sich die der sich wandelnden Technikbewertung zugrundeliegenden Beunruhigungen nicht allein auf abstrakte Gefahrenlagen beziehen. Sie haben ihre Ursache auch in erlebbaren Betroffenheiten, wie etwa einer zunehmenden Umweltverschmutzung oder technikinduzierten Veränderungen der Arbeitsorganisation im Kontext eines sich in der Bundesrepublik Deutschland abzeichnenden wirtschaftsstrukturellen Wandels (Renn 1986: 49). Die darauf abstellenden, mehr oder minder ausdrücklichen, Akzeptanzvorbehalte sind dabei wenig eindeutig, sondern beziehen sich vielmehr auf eine Gemengelage differierender Bewertungen der Bürger im Hinblick auf die unterschiedlichsten Technologien, der Glaubwürdigkeit von politischen Entscheidungsträgern und (wissenschaftlichen) Experten (Petermann/Scherz 2005: 45), sowie sich mit ihnen verbindender „rivalisierende[r] Wertideale“ (Oldemeyer 1988: 42).

Für ein Verständnis des Konzepts der Akzeptanz befördert dies die Erkenntnis, dass Akzeptanz mit den etwa in den Konzepten der Legitimität und Legitimierung angelegten formalen Gehorsamsforderungen „kraft Tradition, qua Institution oder aufgrund formaler Legitimation“ bricht (Lucke 1996a: 474). Akzeptanz, so Lucke (1995: 67) ist vielmehr faktisch nicht erwart-

bar, da sich ihre Bedingungen ebenso wenig aus überindividuellen Gehorsamsgründen ableiten, noch auf die für eine rechtmäßige Herrschaft[25] geltenden, das heißt in den legitimierten Prinzipien verankerte Anerkennung von Entscheidungen – etwa aufgrund ihrer Übereinstimmung mit „Gesetzen, Verfassungen, Prinzipien oder aufgrund ihrer Leistungsfähigkeit für allgemeine Ziele“ (Fuchs-Heinritz 1995a: 396), reduzieren lassen. Nach Lucke (1995), die ihre Definition der Akzeptanz eng an die Herrschaftssoziologie Max Webers und auch semantisch stark an seine Bestimmung von Herrschaft anlehnt, handelt es sich bei der Akzeptanz lediglich um die

> „*Chance*, für bestimmte Meinungen, Maßnahmen, Vorschläge und Entscheidungen bei einer identifizierbaren Personengruppe ausdrückliche oder stillschweigende Zustimmung zu finden und unter angebbaren Bedingungen aussichtsreich auf deren Einverständnis rechnen zu können.“ (ebd.: 104, Herv. hinzugefügt)

Akzeptanz beschreibt in diesem Sinne auch eine (kritische) Haltung und Form der Bezugnahme innerhalb eines gesellschaftlichen Verhältnisses, weil sich in Unbehagen und Protest äußert, was in einer Gesellschaft an Entscheidungen noch angenommen und an Betroffenheiten nicht mehr länger hingenommen, geduldet und insofern ‚akzeptiert‘ werden könne. So gilt denn auch in demokratischen Systemen der (politische) Protest als Form von Teilhabe, „mit der die Herrschenden zu einer Änderung der Politik oder politischer Entscheidungen veranlasst werden sollen“ (Fuchs-Heinritz 1995b: 525). Lässt sich daraus ableiten, dass in der partizipativen Demokratie, „nicht mehr nur der Staat und seine Verwaltung […] für das Gemeinwohl verantwortlich“ sind (Würtenberger 1996: 24), dann stellen sich jene Fragen der Annahme, Hinnahme oder Ablehnung von Entscheidungen für die gesamte „Abstimmungsgesellschaft“ (Lucke 1995). Ihre Relevanz erlangt die Idee der Akzeptanz folglich in dem Moment, so Lucke weiter (1995: 11f., 1996b: 222), in dem ihr Gegenteil theoretisch in der *Öffentlichkeit* denk- und (er)lebbar ist, das heißt jene *Anerkennung*, in Form „qualifizierter Nichtakzeptanz“ (Lucke 1996a: 473) in legitimer Weise nicht nur versagt bleiben kann, sondern auch immer wieder praktisch vorenthalten wird.[26] Die Rede über Akzeptanz erweist sich insofern als Bezugnahme auf eine „kritische Haltung“ und „reflektierte Unfügsamkeit“ (Foucault 1992: 15). Fragen der Akzeptanz stellen sich regelmäßig und insofern immer wieder aufs Neue auf so unterschiedliche Bezugsobjekte wie technische Objekte, Dinge des alltäglichen Gebrauchs, Meinungen, Einstellungen, Lösungsvorschläge, Themen, Probleme, politische Maßnahmen, Personen oder Personengruppen, Berufe oder Milieus (Lucke 1995: 89). Bei der Akzeptanz handelt es sich folglich

[25] Unabhängig davon, ob es sich nun etwa um politische Bewegungen oder Institutionen handelt.
[26] So ist etwa der sogenannte „Akzeptanzvorbehalt“ institutionalisierter Teil der politischen Kultur.

> „um einen hoch brisanten Begriff der politischen, der Rechts- und Alltagssprache sowie der Kultur eines Landes […], in dem sich die Fragen nach den Ursachen, Entstehungsgründen, Erscheinungsformen und Folgen solcher Entwicklungen nicht mehr nur als *begriffliches* oder rein sprachliches Akzeptanzproblem stellen." (ebd.: 38, Herv. i.O.).

Gleichwohl und vielleicht auch deswegen herrscht in der mittlerweile stark differenzierten Akzeptanzforschung weder Einigkeit über den Modus von Akzeptanz, noch darüber, welche als ihre wesentlichen Bedingungen gelten (vgl. ebd.: 34ff.).

1.2.2 Akzeptanzforschung: Konzeptionelle Zugriffe

Es gilt gemeinhin als schwierig ‚die' Akzeptanz sowohl theoretisch als auch empirisch zu fassen. Bereits im alltäglichen Sprachgebrauch ist, wie Doris Luckes (1995: 35ff., 74ff.) begriffliche Analyse zeigt, Akzeptanz aufgrund zahlreicher Variationen und vielzähliger bildungs- und umgangssprachlicher Synonyme durch eine hohe semantische Uneindeutigkeit gekennzeichnet. Dies bringt ihr zuweilen den Vorwurf ein gar ein „amorphes" (vgl. Ullrich 2008: 19), das heißt ein grundsätzlich für eine soziologische Verwendung zu weit gefasstes und diffuses, Konzept (vgl. Weber 1972: 28) zu sein, was nicht zuletzt in den zahlreichen (inter-)disziplinären Zugriffen auf die Akzeptanz seinen Beleg zu finden scheint (vgl. z.B. Petermann/Scherz 2005).

Eine etablierte Differenzierung der ansonsten mittlerweile nur schwerlich zu strukturierenden Akzeptanzforschung (ebd.) bildet die Unterscheidung zwischen individueller und gesellschaftlicher Akzeptanz. Mit dieser wird zugrunde gelegt, dass sich Fragen der Annahme zunehmend für eine Vielzahl unterschiedlicher Personengruppen in Bezug auf vielfältige (technische) Objekte stellen. Richten sich „individuelle" Akzeptanzfragen auf Technologien, denen im Sinne „konsumtiver Akzeptanz" (Renn 1986: 45) Kauf- oder Entscheidungen für die Nutzung am Arbeitsplatz (ebd.) zugrunde liegen, wird im Rahmen der gesellschaftlichen oder „sozialen" Akzeptanz (vgl. z.B. Kollmann 1998) dagegen vom individuellen Nutzer abstrahiert. Dem Konzept der „Akzeptanz als Nachbar" (Renn: 1986: 45) entsprechend nimmt eine solche Forschungsrichtung eine gesamtgesellschaftliche Betroffenheit von sogenannten Großtechnologien in den Fokus.

1.2.2.1 Individuelle Akzeptanz

An Fragen der individuellen (Technik-)Akzeptanz sind zunächst vor allem wirtschaftswissenschaftlich orientierte Untersuchungen interessiert. Eine solche, seit den 1960er Jahren aus der Absatzlehre (Dethloff 2004: 17) hervorgehende und sich in den 1970er und 1980er Jahren etablierende, ökonomische Akzeptanzforschung (Kollmann 1998: 54ff.) ist im Wesentlichen mit den Kriterien der Befürwortung und Ablehnung von Produkten befasst. In der Vorstellung ein technisches Erzeugnis besitze bestimmte, gleichwohl aus der Nutzerperspektive variable, Eigenschaften, die sich von den Herstellern eindeutig (re-)produzieren lassen, zielen die Bemühungen darauf, als akzeptanzrelevant erachtete Einstellungen potentieller Nutzer gegenüber dem Technologieprodukt zu erfassen. So ist Forschung zur Akzeptanz dann auch vor allem Einstellungsforschung. Unabhängig von der durchaus uneinheitlichen Verwendung des Begriffes in der Akzeptanzforschung zeichnet sich die Einstellungsforschung dadurch aus, dass sie von der Grundannahme geleitet ist, dass Einstellungen dem sozialen Handeln vorausgehen (vgl. Meinefeld 1977: 17) und, zumindest indirekt, der Messung zugänglich sind, wie es vor allem aus der Sozialpsychologie stammende Theorien (z.B. Fishbein/Ajzen 1975) nahelegen. Gemäß dieser hängt die Akzeptanz bzw. affirmative Einstellung einer Person gegenüber einem Objekt davon ab, welche subjektiven Annahmen sich mit bestimmten Attributen des Objektes verbinden. Ist die Untersuchung des Zusammenhangs zwischen mentalen Zuständen, seien es Annahmen, wissensbasierte Überzeugungen (die sogenannte kognitive Dimension der Akzeptanz) oder Gefühle, das heißt affektive Haltungen in Bezug auf ein Objekt und eines sich daran ausrichtenden sozialen Handelns (Verhaltens- oder konativer Aspekt) der wesentliche Ausgangspunkt innerhalb der Akzeptanzforschung, erweist sich das Einstellungskonzept für die wirtschaftswissenschaftlich orientierte Akzeptanzforschung aber auch für die Möglichkeit der Handlungsprognose und gezielten Einflussnahme auf soziales Handeln als zentral (zur sozialen und politischen Bedeutung der Einstellung vgl. Meinefeld 1977: 17ff.). So gilt seit den frühen 1980er Jahren eine an bereits implementierten Technologien ausgerichtete Akzeptanzforschung für eine ‚akzeptanzorientierte' Technikgestaltung nicht länger als hinreichend. Die an individueller Akzeptanz orientierte Forschung folgt zunehmend auch einer gestaltenden Zielsetzung (vgl. Manz 1983), um vor allem das aus betriebswissenschaftlicher Perspektive mit fehlender Nutzerakzeptanz (im Sinne einer Nicht-Nutzung) einhergehende Risiko von Fehlinvestitionen in Innovationen zu senken (vgl. Kollmann 1998). Unter Einbezug akzeptanzrelevanter Faktoren, die sozialpsychologische Theorien[27], Ansätze

[27] Hierzu gehören z.B. die „Theory of Reasoned Action" von Fishbein/Ajzen (1975) oder die „Theory of Planned Behaviour" von Ajzen (1985).

der Diffusions- und Adoptionsforschung (z.B. Rogers 2003) oder sogenannte Technologieakzeptanzmodelle (zum Beispiel das „Technology Acceptance Model“ von Davis 1989 oder Venkatesh/Davis 2000) bereitstellen – und in deren Mittelpunkt der rationale, bilanzierende Akteur steht –, zielt diese Forschung darauf, Nutzereinstellungen zu antizipieren, um auf dieser Grundlage die ‚widerständigen‘ Aspekte eines Produktes, etwa im Hinblick auf Kompatibilität, Benutzerfreundlichkeit und Erlernbarkeit, zu minimieren, um so Konsum bzw. Nutzung durch eine hohe ‚Nützlichkeit‘ maximieren zu können (vgl. z.B. Degenhardt 1986). Damit geben wirtschaftswissenschaftliche Studien zur Akzeptanz vor allem Auskunft über die Wahrscheinlichkeit einer künftigen Nutzung.

1.2.2.2 Gesellschaftliche Akzeptanz

Fragen der gesellschaftlichen Akzeptanz, das heißt zu einer im weitesten Sinne gesamtgesellschaftlichen An- bzw. Hinnahme von sogenannten Groß- und Risikotechnologien, wenden sich unterschiedliche Forschungsrichtungen zu, unter anderem die Meinungsforschung (Demoskopie) (vgl. Jaufmann 1999), die auf das Erfassen von Einstellungen gegenüber neuen Technologien spezialisiert ist, die sozialwissenschaftliche Risikoforschung (vgl. Gloede/Hennen 2005: 3) sowie an deren Schnittstelle seit den 1980er Jahren die akzeptanzorientierte Techniksoziologie, die Technikfolgenabschätzung (TA). Letztere hinterfragt nicht nur die von den Meinungsforschungsinstituten als technikfeindlich deklarierten Einstellungen der Bürger. Unter Bezug auf Ergebnisse der sozialwissenschaftlichen Risikoforschung relativiert sie zudem die Annahme einer irrationalen, dem Risikokalkül von Experten unterlegenen, Wahrnehmung von Laien (ebd.: 5, vgl. Wiedemann/Mertens 2005). Demgegenüber betont sie, dass die alltagsweltliche Beurteilung von Risiken etwa nicht von statistischen Erwartungen abhängt, sondern es vor allem qualitative und situative Momente sind, die für die Risikowahrnehmung ausschlaggebend sind (vgl. Luhmann 1997: 328ff.): Die Bereitschaft, sich auf Risiken einzulassen, ist danach etwa dadurch bestimmt, wie vertraut eine in Frage stehende Unsicherheit ist, aber auch davon, ob man sich in der Lage fühlt, eine solch prekäre Situation zu beherrschen oder den Schadensfall durch Hilfen, Versicherungen etc. abzudecken (vgl. dazu Bechmann 1997: XIII, Bonß 1995: 302). So finden sich allein aufgrund der unterschiedlichen Zurechnung von Risiken als auch zu den Möglichkeiten ihrer Vermeidung innerhalb der Bevölkerung andere Einschätzungen zu diesen als in der Politik, und insofern „bei Laien andere als bei Experten.“ (Luhmann, 2003: 123, vgl. auch ebd. 1997: 331) Danach wird, wie Luhmann (ebd.: 11, 122ff.) die Ergebnisse der Risikoforschung zusammenfasst, folglich auch

die „Katastrophenschwelle“, die es nötig macht einzugreifen, „sehr verschieden gezogen […] je nachdem, ob man am Risiko als Entscheider oder als von riskanten Entscheidungen Betroffener beteiligt ist“.

Obwohl die Bürger mit einer solchen Hinwendung der Forschung zu Interpretations- und Aneignungsprozessen von Technologien nunmehr als ‚Betroffene‘ Eingang in die theoretische Debatte um die alltägliche Auseinandersetzung mit Technik und ihren Wandel erhalten, ihre Wissensbestände gar in Konkurrenz zu jenen der Experten (Wiedemann/Mertens 2005: 38) treten, wendet sich die Technikakzeptanzforschung gleichwohl zunehmend ab von den der Akzeptanz vorausgehenden bzw. diese konstituierendem Bedingungen (vgl. zu Ausnahmen z.B. Rammert 1988, Hörning 1988), etwa den Zuschreibungs- und Aushandlungsprozessen, Deutungs- und Umgangsweisen mit Technik sowohl von Experten als auch von Laien. Stattdessen ist sie daran orientiert, die Risiken ohnehin eingeführter bzw. einzuführender Technologien bereits im Vorhinein auf ein ‚akzeptables‘ Maß zu begrenzen. Risikokommunikation wird zum „Zauberwort“ in der Debatte um die Akzeptabilität technischer und anderer Risiken (Renn 1991: 193) und in den 1980er Jahren gilt die Erhebung individueller Risikoeinstellungen mit dem Ziel, diese durch ein Mehr an und ‚bessere‘ Informationen zu beeinflussen, als aussichtsreich, um eine Annäherung der Laienperspektiven an jene der Experten herzustellen (Gloede/Hennen 2005: 6). Stellvertretend für andere lässt sich das hier zugrundeliegende Verständnis von Akzeptanz, als einem weitestgehend herstellbaren Zustand von Konfliktfreiheit, mit Ortwin Renn (1986: 44) fassen, wonach diese

> „mehr [ist] als passive Duldung der ‚von oben‘ verordneten technischen Neuerungen. Vielmehr soll hier unter Akzeptanz die positive Aufnahme einer Veränderung der physischen Umwelt verstanden werden.“

Gilt in diesem Verständnis die „bewußte Auseinandersetzung mit dem Gegenstand der Veränderung“ (Renn: ebd.), im Sinne eines als notwendig erachteten Einbezugs der Bürgerperspektiven (Grunwald 2005: 2), als ihre Voraussetzung, verändert sich die Akzeptanzpolitik in den 1990er Jahren von der reinen Informationspolitik hin zum Konzept eines „Public understanding of Science and Technology“ (Barben 2010b: 277, vgl. Gloede/Hennen 2005: 6). Der Idee einer partizipativ orientierten Technikentwicklung folgend, gilt es nun, Akzeptanz durch den „deliberativen“ Austausch zwischen Experten- und Laienperspektiven (vgl. Renn/Zwick 1997: 98f., dazu auch Petermann 1999: 34f.) herzustellen. An diese Orientierung richtet sich seit den 1990er Jahren dann auch ein Vorschlag, unter dem Begriff der Akzeptabilität (Grunwald 2005: 54 mit Bezug auf Gethmann/Mittelstraß 1992, Gethmann/Sander 1999), und somit der Übersetzung der ‚Sozialverträglichkeit‘ in Kriterien ethischer Rechtfertigbarkeit von

Technik, Fragen der Akzeptanz letztlich von den Wahrnehmungen der Akzeptierenden abzukoppeln. Doris Lucke (1995: 106) beschreibt die Akzeptabilität als einen Begriff, der sich auf gesellschaftlich übergeordnete Prinzipien bezieht und mit dem „die prinzipielle Erwartbarkeit mehrheitlichen Einverständnisses auf der objektivierbaren Grundlage allgemein anerkannter und rational begründeter gesellschaftlicher, politischer, wirtschaftlicher etc. Oberziele“ bezeichnet wird. Gilt Akzeptanzverhalten als in seinen Entstehungsbedingungen zu komplex und seine Prognose daher schwerlich leistbar, zielt die zwischen präventiver Implementations- und kurativer Begleitforschung zu verortende Forschung (vgl. Manz 1983: 6ff.) vor allem darauf, die Sozialverträglichkeit von Technologien zu gewährleisten: entweder dadurch, dass sie „sich funktional in eine bestehende Sozialstruktur einpflanzen lässt (*evolutionärer Wandel*) oder eine gegebene Sozialstruktur so verändern zu können, dass sie funktional in die neue Sozialstruktur passt (*revolutionärer Wandel*).“ (Endruweit 2011: 6, Herv. i.O.) Eine Orientierung an Akzeptabilität bedeutet demnach, eine gesellschaftliche Einigung über den Risikograd einer Technologie zu erzielen und Akzeptanz insofern primär mit Bezug auf ihre „ethische[n] Verantwortbarkeit“ (Renn 2005: 29) zu bestimmen.

1.2.3 Die Akzeptanz von Biometrie: Ein Blick in die Empirie[28]

In der Tradition einer vorangehend als tendenziell am Konsens orientiert charakterisierten Akzeptanzforschung zielt auch die Forschung zur Akzeptanz biometrischer Technologien in der Regel darauf ab, die Grenzen des (gerade noch) Akzeptablen auszuloten. Dies geschieht zunächst auf einer Makroebene: Ob die Nutzung von Fingerabdrücken etwa in nationalen Identitätsdokumenten zumutbar ist, beschäftigt die Forschung zunächst angesichts eines identifizierten „Demokratiedefizit“ (Hornung 2007: 153) ihrer Einführung. Weniger die Akzeptanz als vielmehr den Prozess der Entscheidungsfindung befragend richtet sie ihr Augenmerk rechtstheoretisch auf Gesetzgebungsverfahren und neue Rechtsnormen (z.B. Hornung 2004, 2005, ausführlich zur Entscheidungsfindung auf EU-Ebene vgl. Aus 2008). In diesem Zusammenhang beklagt das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag in seinem 2. Sachstandsbericht zu Biometrie und Ausweispapieren (BT-Drs. 15/4000: 58) 2004 einen kaum vorhandenen öffentlichen Diskurs und fordert mit Blick auf die Akzeptanz der Technologie ein, vorab die Akzeptabilität der faktischen Entscheidungsinhalte in öffentlichen

[28] Eine zusammenführende Betrachtung von Untersuchungen zur Akzeptanz von Sicherheitsmaßnahmen ist von der Autorin bereits im Rahmen der Untersuchung „Die Gesellschaftliche Konstruktion von Sicherheit. Zur medialen Vermittlung und Wahrnehmung der Terrorismusbekämpfung“ (Krasmann et al. 2014: 79ff.) vorgenommen worden und findet in überarbeiteter Form Eingang in die nachfolgenden Ausführungen.

Beteiligungsverfahren daraufhin zu prüfen, wieviel die Bürger bereit seien, an Eingriffen in ihre Freiheit für den avisierten Sicherheitszweck der Maßnahme hinzunehmen.

Den Auftakt der Forschung zur Biometrie bilden gleichwohl staatlich geförderte Projekte mit der primären Zielsetzung, den Rahmen des technisch Möglichen und wirtschaftlich sinnvollen Einsatzes auszuloten. Für die um die Jahrtausendwende einsetzenden staatlich geförderten Pilotprojekte, etwa die durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) initiierte und gemeinsam mit dem Bundeskriminalamt (BKA) durchgeführte „Vergleichende Untersuchung biometrischer Identifikationssysteme – BioIS“ (BT-Drs. 14/1405, Büllingen/Hillebrand 2000)[29] oder das mit 2,5 Millionen Euro durch das Bundesministerium für Wirtschaft und Technologie (BMWi) geförderte Projekt „BioTrust“[30], deren erklärtes Ziel es war, wie bereits in Kapitel 1.1.1 dargestellt, den Markt für kommerzielle Biometrieprodukte zu öffnen (BT-Drs. 14/1405: 2), erschließen sich diese Chancen vor allem in der Terminologie der sicheren Alltagspraktikabilität (Petermann/Sauter 2002: 42). Im Projekt „BioIS“ etwa, das anhand eines Praxisvergleiches verschiedener biometrischer Systeme Evaluierungs-, Normierungs- und Zertifizierungskriterien für biometrische Verfahren zu entwickeln suchte, wurden „zehn auf dem deutschen Markt erhältliche biometrische Geräte auf Alltagstauglichkeit und Verwendbarkeit für sicherheitskritische Anwendungen“ (ebd.) untersucht. Wurden nur zwei Geräte für ‚alltagstauglich‘ befunden (ebd.), dann vor allem deshalb, weil die Technologie offenbar wesentlichen Sicherheitsanforderungen nicht genügte. Gleichwohl suggerierten die Befunde einer an den Praxistest anschließenden Akzeptanzbefragung eine erfolgsversprechende Vermarktungsstrategie, die statt auf Sicherheits- auf Convenience- bzw. Annehmlichkeitsaspekte setzten solle (vgl. Büllingen/Hillebrand 2000: 342) – prospektive Akzeptanz- resp. Marktchancen, die gleichwohl mit dem ‚Ereignis 9/11‘ vorrübergehend ‚vergessen‘ wurden.

Ob sich biometrische Technologien wie die Fingerbildauthentifizierung erfolgreich als sicheres und gleichsam praktikables Produkt auch in spezifischen privatwirtschaftlichen Anwendungen implementieren lassen, ist zudem etwa von Weber (2008) für den Bereich der Zugangssicherung zum Arbeitsplatzrechner bzw. Al-Harby et al. (2010) für das Onlinebanking im arabischen Raum oder auch von Clodfelter (2010) für den Einzelhandel in den USA untersucht worden. In der Logik die Akzeptanz durch die prospektive Erfassung ihrer Akzeptabilität präventiv zu modulieren werden – neben diesen ökonomisch orientierten und auf zukünfti-

[29] Das Projekt begann 1999 und endete im darauffolgenden Jahr.

[30] Laufzeit 1999-2002. Ganz im Sinne kundenorientierter Anwendungen – Mitinitiator des Projektes war die Sparkassen-Finanzgruppe – wurde hier die biometrische Identifizierung im Zahlungsverkehr untersucht (BT-Drs. 14/1405: 2).

ge Marktchancen biometrischer Technologien gerichteten Untersuchungen –, auch die verbindlich zu implementierenden Fingerabdrucktechnologien im Hinblick auf ihre Adoptionsbedingungen untersucht, etwa von Ng-Kruelle et al. (2006), die diese für den biometrischen Reisepass in unterschiedlichen Ländern erforschten.

Ist die Akzeptanz von Biometrie demnach noch eher selten untersucht worden, so zeigt sich gleichwohl in den letzten Jahren im Kontext der Sicherheitsforschung und nicht zuletzt vor dem Hintergrund der zunehmenden Fördertätigkeit der Bundesregierung im Themenfeld der Sicherheit (vgl. Gerhold et al. 2012: 13), dass sich das Forschungsinteresse verstärkt auf die Fragen der Akzeptanz von zu implementierenden Sicherheits- und Kontrolltechnologien richtet. Die Akzeptanz von Sicherheitsmaßnahmen im Flughafenumfeld wurde zum Beispiel im Rahmen zweier vom Bundesministerium für Bildung und Forschung (BMBF) finanzierter Projekte untersucht. Das Projekt „Sicherheit im öffentlichen Raum" („SIRA", Teilprojekt 7, Bug/Wagner 2015)[31] befragte Flugpassagiere zu faktisch installierten Sicherheitsmaßnahmen.[32] Ein weitere Untersuchung zur Einschätzung der Bevölkerung zu (intelligenter) Videoüberwachung an Flughäfen wurde im Projekt „Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme" („APFel", Feltes et al. 2013)[33] vorgenommen. Auch für den Fährverkehr stellten sich Fragen der Akzeptanz von Sicherheitsmaßnahmen, die infolge der Terroranschläge am 11. September 2001 durch den International Ship and Port Facility Security Code (ISPS-Code)[34] sowie die EU-Gesamthafenrichtlinie erhöht wurden. Diese untersuchte das BMBF-Projekt „Verbesserung der Sicherheit von Personen in der Fährschifffahrt" (VESPER+, Schlepper et al. 2015)[35].

[31] Das Teilprojekt 7 des zwischen August 2010 und Juli 2013 durchgeführten Projektes umfasste aufgrund seines in vergleichender Perspektive angelegten Konzepts auch die Untersuchung der Akzeptanz der Vorratsdatenspeicherung im Sozialraum Internet (Bug/Münch 2012).

[32] Die Studie umfasste unter anderem eine Repräsentativbefragung von 799 Flugpassagieren, das heißt Personen, die im Durchschnitt mindestens einmal pro Jahr fliegen, zu ihren Einschätzungen von Sicherheitsmaßnahmen (im Allgemeinen) und ihrem Sicherheitsgefühl infolge der installierten Maßnahmen.

[33] Im Rahmen der im September 2010 am Flughafen Hannover durchgeführten standardisierten Befragung wurden 1.400 Flugpassagiere nach dem Nutzen (z.B. zur individuellen kognitiven Risikowahrnehmung), den instrumentellen Folgen des Einsatzes (das heißt zur kriminalpräventiven Wirkung) und den Kosten der Maßnahme, wie z.B. individuellen Konsequenzen für die persönliche Freiheit (Datenschutz, Gefühl des Unwohlseins) befragt.

[34] „Als Maßnahme der präventiven Gefahrenabwehr verpflichtet der ISPS-Code die maritime Wirtschaft in Deutschland auf der Basis von Risikobewertungen technische und personelle Instrumente (z.B. Zugangskontrollen und/ oder Überwachungsmaßnahmen) zur Abwehr externer Bedrohungen in die Arbeitsprozesse auf Schiffen und in Hafenanlagen zu integrieren. Der ISPS-Code findet seine Anwendung universell auf allen international verkehrenden Schiffen und unzähligen Hafenanlagen weltweit. Gefahrenstufe 2 findet Anwendung, sobald und solange ein erhöhtes Risiko eines sicherheitsrelevanten Ereignisses besteht." (Krasmann et al. 2014: 86)

[35] Die Befragung von 766 Fährpassagieren im Ostsee-Verkehr zwischen Deutschland und Skandinavien im Sommer 2012 erfolgte im Rahmen des Teilprojektes „Gesellschaftliche und wirtschaftliche Auswirkungen neuer Sicherheitsmaßnahmen im Fährverkehr".

Wurde nun die Einführung von Fingerabdruckdaten in die Identitätspapiere politisch zumeist als konsequente oder gar erforderliche Antwort auf eine neue Bedrohungslage dargestellt, wird die Akzeptanz neuer Technologien der Sicherheit und Kontrolle dann auch dahingehend untersucht, inwiefern solche Diskurse tatsächlich ihren Widerhall in der Wahrnehmung der Bürger finden. Im von der DFG geförderten Projekt „Der ‚überwachte Bürger' zwischen Apathie und Protest", das seinen Fokus auf eine Vielzahl seit 2001 faktisch implementierter staatlicher Kontroll- und Überwachungstechnologien richtet, wurde unter anderem die Akzeptanz der neuen, mit Fingerabdruckdaten ausgestatteten, elektronischen Ausweisdokumente (Lüdemann/Schlepper 2013) untersucht.[36] Eine vergleichbare Zielrichtung liegt auch der Untersuchung von Pietsch und Fiebig (2011) zugrunde, die, wenngleich die Autoren selbst den Begriff der Akzeptanz nicht verwenden, den Einfluss von Bedrohungsgefühlen auf die „Unterstützung bestimmter erweiterter Mittel der Terrorabwehr" (ebd.: 268) prüft. Sie beziehen sich hierzu auf Daten der Bevölkerungsumfrage des Sozialwissenschaftlichen Instituts der Bundeswehr 2010 und untersuchten die Bewertung von (12) unterschiedlichen, sowohl faktischen als auch zum Zeitpunkt der Erhebung lediglich theoretischen, das heißt nicht installierten, Maßnahmen zur Terrorismusbekämpfung. Dazu gehörte auch die zentrale Erfassung der Fingerabdrücke in einer Zentraldatei zum Zweck der Terrorismusbekämpfung.

Ein Vergleich der Ergebnisse zur Akzeptanz der Fingerabdrucktechnologie, die in den Untersuchungen neben anderen Maßnahmen erhoben wird, wird trotz der eher spärlichen Forschungslage durch eine Reihe von Faktoren erschwert: die Studien unterscheiden sich nicht nur hinsichtlich der jeweils in den Blick genommenen Technologien und so auch mit den je avisierten und/oder faktischen Nutzungen. Adressiert werden neben unterschiedlichen Anwendungsszenarien zudem zukünftige Verhaltensabsichten sowie Bedingungen einer bereits unterstellten Akzeptanz. Kennzeichnet die Forschung gleichwohl, dass sich die Frage der Akzeptanz im Wesentlichen in einer Form stellt, wonach ihre bedingenden oder erklärenden Faktoren als a priori erfassbar gelten, dann unterscheiden sich die Studien zur Akzeptanz von Fingerabdrücken in den Ausweispapieren bzw. Fingerabdruckverfahren auch dahingehend, dass sie, einerseits, Akzeptanz als eine Frage der „Bewertung" oder Zustimmung der in Frage stehenden Technologie konzipieren und entsprechende Faktoren prüfen (Pietsch/Fiebig 2011, Lüdemann/Schlepper 2013). Andererseits suchen Studien (die Grenze der) Akzeptanz nicht nur im Maß der Zustimmung zu einer konkreten Maßnahme, sondern auch direkt über die

[36] Die im Oktober 2009 durchgeführte standardisierte Telefonbefragung zu staatlichen Überwachungsmaßnahmen beruhte auf einer repräsentativen Stichprobe von 2.176 in Privathaushalten lebenden Personen ab 18 Jahren. Untersucht wurde der Einfluss punitiver Einstellungen, der Furcht vor Kriminalität und Terrorismus sowie des erwarteten „Nettonutzens" der Technologien auf die individuelle Bewertung der in der Befragung vorgelegten Maßnahmen (Lüdemann/ Schlepper 2013).

einstellungsorientierte Attribuierung von Vor- und Nachteilen der Technologie (anhand entsprechender Technologie-Akzeptanz-Modelle) zu ermitteln (vgl. Weber 2008, Al-Harby et al. 2010). Mitunter wird die prospektive Akzeptanz in Umfragen durch Rangfolgen nützlicher Aspekte untersucht (z.B. Clodfelter 2010) oder es wird explizit die Akzeptabilität nicht allein durch Befragungen, sondern auch auf der Basis von Medieninhaltsanalysen antizipiert (Ng-Kruelle et al. 2006). Zuletzt beziehen sich die Studien, im Rahmen der Sicherheitsforschung, zudem auf eine Vielzahl unterschiedlicher Maßnahmen. So werden in der Studie von Lüdemann und Schlepper (2013) auch die Bewertung des Online-Zugriffs auf digitalisierte Lichtbilder, das Kontenabrufverfahren, die Vorratsdatenspeicherung von Telefon- und Internetverbindungsdaten, die Online-Durchsuchung, die Einrichtung der Antiterrordatei und der Passagierdatenspeicherung untersucht (vgl. auch Pietsch/Fiebig 2011). Aus diesem Grund werden, statt die einzelnen Untersuchungen in Gänze vorzustellen, nur einige Aspekte und Ergebnisse der Studien nachfolgend betrachtet.

In der Studie von Lüdemann und Schlepper (2013) wird explizit die Bewertung der biometrischen Ausweispapiere untersucht. Um zu klären, in welchem Maß die Bürger einzelne Kontroll- und Überwachungstechnologien akzeptieren, wurde zunächst die subjektive Einschätzung der einzelnen Maßnahmen durch die Frage danach, wie gut oder wie schlecht sie diese einzelnen Maßnahmen finden, erhoben. Als Antwortmöglichkeiten vorgegeben wurden: *sehr gut*, *eher gut*, *eher schlecht* oder *sehr schlecht* (vgl. Tabelle 1).

Tabelle 1: Wie bewerten die Bürger die folgenden Kontroll- und Überwachungstechnologien?

	sehr gut	*eher gut*	*eher schlecht*	*sehr schlecht*	*Mittelwert*
Biometrische Ausweisdokumente	691 32,2%	979 45,6%	323 15,0%	155 7,2%	3.03
Antiterrordatei	604 28,2%	1037 48,4%	364 17,0%	139 6,5%	2.98
Online-Zugriff auf digitalisierte Lichtbilder	598 27,9%	1044 48,6%	345 16,1%	160 7,5%	2.97
Erfassung von Passagierdaten	462 21,5%	971 45,1%	527 24,5%	192 8,9%	2.79
Zugriff auf Bankdaten	378 17,5%	808 37,5%	703 32,6%	265 12,3%	2.60
Online-Durchsuchung	330 15,3%	655 30,4%	632 29,4%	535 24,9%	2.36
Vorratsdatenspeicherung	188 8,7%	475 22,0%	776 36,0%	719 33,3%	2.06

Quelle: Krasmann et al. 2014: 81 (N = 2.176), Herv. hinzugefügt

In der Befragung des Sozialwissenschaftlichen Instituts der Bundeswehr 2010 wurde hingegen die jeweilige Zustimmung bzw. Ablehnung zu der Frage *Um die Menschen in Deutschland vor den Gefahren des Terrorismus zu schützen, werden verschiedene Maßnahmen erwogen. Sagen Sie mir bitte, ob Sie den folgenden Vorschlägen zur Terrorabwehr zustimmen oder ob Sie diese ablehnen* erfragt (Pietsch/Fiebig 2011: 269, vgl. Tabelle 2).

Tabelle 2: Zustimmung und Ablehnung der Maßnahmen

	stimme zu	*stimme eher zu*	*lehne eher ab*	*lehne ab*	*weiß nicht/ k.A.*
Überführte Terroristen härter bestrafen	78%	13%	4%	3%	3%
Verdächtige Ausländer aus Deutschland ausweisen	65%	19%	9%	5%	2%
Die militärischen Mittel und Möglichkeiten der Bundeswehr auch im Inland nutzen, z.B. zum Schutz von Atomkraftwerken	60%	26%	7%	5%	2%
Mehr Polizisten in der Öffentlichkeit einsetzen	58%	24%	12%	4%	2%
Öffentliche Plätze und Gebäude, z.B. Flughäfen und Bahnhöfe, verstärkt mit Videokameras überwachen	56%	24%	9%	8%	2%
Potentielle Terroristen vorbeugend in Gewahrsam nehmen	56%	23%	10%	7%	4%
Handy- und Internetverbot für Personen, die im Verdacht stehen, Terroranschläge vorzubereiten	45%	23%	13%	12%	7%
Den Verfassungsschutz auf die Bank-, Telefon- und Reisedaten (z.B. Flugverbindungen) von verdächtigen Personen zugreifen lassen	44%	28%	12%	11%	4%
Fingerabdrücke und andere Persönlichkeitsmerkmale von allen Bundesbürgern in einer zentralen Datei erfassen und zur Verbrechensbekämpfung nutzen	40%	17%	15%	24%	4%
Die Möglichkeiten zum Abhören von Telefonen und Privaträumen ausweiten	23%	19%	24%	29%	5%
Online-Durchsuchungen von privaten Computern aller Bundesbürger ermöglichen	16%	12%	24%	43%	6%
Von Terroristen gekaperte Flugzeuge im Notfall abschießen, auch wenn dabei unschuldige Passagiere getötet werden	11%	11%	24%	44%	11%

Quelle: Pietsch/Fiebig 2011: 269 (N = 3.026), Herv. hinzugefügt

Bewerten 77,8 Prozent der Befragten die Einführung des ePasses, das heißt eines Reisepasses mit biometrischem Passbild und digitalisiertem Fingerabdruck, in der Studie von Lüdemann und Schlepper (2013: 155) mit *gut* bis *sehr gut* (vgl. Tabelle 1), erreicht eine vom Dokument abgekoppelte zentrale Speicherung von Fingerabdrücken aller Bundesbürger eine vergleichsweise geringere Akzeptanz. So *lehnen* 39 Prozent der Befragten in der Studie von Pietsch und Fiebig (2011: 269) eine zentrale Speicherung unter der Voraussetzung, dass diese „zur Verbrechensbekämpfung“ genutzt wird, *ab* bzw. *eher ab* (vgl. Tabelle 2).

Und auch für den Zusammenhang von Unsicherheitsgefühlen und Akzeptanz zeigen sich Unterschiede: Während Lüdemann und Schlepper (2013: 158) etwa in ihrer Studie zeigen, dass Personen mit einer hohen Furcht vor terroristischen Anschlägen staatliche Sicherheits- und Kontrollmaßnahmen wie elektronische Identitätspapiere mit Fingerabdruckdaten positiver bewerten, weisen Pietsch und Fiebig (2011: 274) die Wirkung eines individuellen Bedro-

hungsgefühls (mittels einer Faktorenanalyse) trotz allgemeiner Bedrohungswahrnehmungen auf die Zustimmung hingegen als relativ gering aus.[37] Erfahren in der Studie von Lüdemann und Schlepper (2013: 155) nun die biometrischen Ausweisdokumente die vergleichsweise höchste Akzeptanz im Sinne einer mehrheitlich positiven Bewertung, dann, so ein weiteres Ergebnis der Studie, weil ihr Nutzen für die Sicherheit das Risiko der missbräuchlichen Datenverwendung und mithin der Überwachung überwiegt.[38] Erweisen sich den Studien zufolge Nützlichkeiten, wie etwa Sicherheitsgewinne, als akzeptanzbedingende Faktoren, sind folglich Risiken ihre Kehrseite. Die quantitativen Untersuchungen nähern sich der Frage der Nachteile empirisch, indem den erfragten Sicherheitsgewinnen die (gefühlten) „Kosten" (vgl. Lüdemann /Schlepper 2013) oder Risiken, etwa eine fehlende Funktionalität des technischen Systems, hygienische Bedenken bei seiner Benutzung oder der potentielle Missbrauch der Daten (vgl. Weber 2008) gegenübergestellt werden. So wurde im Hinblick auf die kognitive Ebene der Akzeptanz in der Studie von Lüdemann und Schlepper (2013) erhoben, ob die Maßnahmen von den Befragten eher mit Sicherheit oder Überwachung assoziiert werden (vgl. Tabelle 3).

[37] Ähnliche Ergebnisse im Sinne einer vom Großteil der Befragten eher als gering eingeschätzten persönlichen Bedrohung zeigen im Hinblick auf andere Sicherheitsmaßnahmen sowohl Schlepper et al. (2015) als auch Bug und Wagner (2015). Unter anderem deshalb halten Bug und Wagner (2015) die Bewertung der „Zweckmäßigkeit" der Sicherheitsmaßnahmen (im Flughafenkontext) für ein entscheidendes Kriterium für die Akzeptanz. Auf die Frage „Halten Sie die bisherigen Sicherheitsmaßnahmen zur Abwehr von terroristischen Anschlägen rund ums Fliegen für zweckmäßig?" antworteten 23,8 Prozent der befragten Flugpassagiere mit sehr zweckmäßig und 52,7 Prozent mit eher zweckmäßig. Dieses Ergebnis gilt den Autoren dann auch als die entscheidende Erklärung für einen hohen „Zuspruch" zu den Maßnahmen.

[38] Die in der Studie postulierten Zusammenhänge (Ängste, Erfahrungen mit staatlicher Kontrolle, Kosten- und Nutzenerwartungen sowie punitive Einstellungen auf die Bewertung der Maßnahme) wurden anhand eines Strukturgleichungsmodells überprüft (Lüdemann/Schlepper 2013)

Tabelle 3: Bedrohung der Privatsphäre und Empfinden von Kontrollverlusten

Bedrohung der Privatsphäre	
Fühlen Sie sich durch die Maßnahme in Ihrer Privatsphäre verletzt?	17,4% Zustimmung *(ja, auf jeden Fall)*
Gefühl des Kontrollverlusts: Erhebung von Daten	
Haben Sie das Gefühl, die Kontrolle darüber zu verlieren, ob, wann und in welchem Ausmaß Sie vom Staat überwacht werden? (ISIP-Projekt 2009, eigene Berechnungen, N = 2.176)	28,7% Zustimmung (*ja, auf jeden Fall*)
Haben Sie das Gefühl, die Kontrolle darüber zu verlieren, wie Ihre Ausweis-, Telefon-, Passagier- und Bankdaten verwendet und gespeichert werden? (ISIP-Projekt 2009, eigene Berechnungen, N = 2.176)	33% Zustimmung (*ja, auf jeden Fall*)
Gefühl des Kontrollverlusts: Verwendung der erhobenen Daten	
Glauben Sie, dass Behörden Ihre Ausweis-, Telefon-, Bank-, Passagier- und Internetdaten nur zu Zwecken verwenden, denen Sie zugestimmt haben? (ISIP-Projekt 2009, eigene Berechnungen, N = 2.176)	16,7% Ablehnung (*nein, auf keinen Fall*)
Glauben Sie, dass Behörden mit Ihren Ausweis-, Telefon-, Passagier-, Bank- und Internetdaten vertrauenswürdig umgehen? (ISIP-Projekt 2009, eigene Berechnungen, N = 2.176)	15,8% Ablehnung *(nein, auf keinen Fall)*

Quelle: Krasmann et al 2014: 99f.

Auch wenn die Ergebnisse andeuten, dass mit einem Gefühl der Sicherheit, das sich an die Maßnahmen knüpft, nicht zwangsläufig eine unkritische Haltung einhergeht, gehen gleichwohl der Studie nach, vermittelt unter anderem über die Angst vor einem Terroranschlag, „die stärksten Effekte auf die Akzeptanz der neuen Überwachungsmaßnahmen […] von dem erwarteten Nettonutzen dieser Maßnahmen aus." (ebd.: 157) Dies verweist dann auch zurück auf ihre Ausgangsannahme, wonach die massenmediale und politische Problematisierung von Unsicherheitslagen Sicherheitsbedürfnisse und mit ihnen die Akzeptanz neuer Technologien, die auch im Kontext potentieller Überwachungsrisiken diskutiert werden, befördert und dies auch unabhängig des jeweils vorhandenen Wissens über die konkrete Maßnahme.[39] Vergleichbares deuten dann auch die Ergebnisse von Ng-Kruelle et al. (2006: 18f.) an, die Medienarstellungen als Stellvertreter für gesellschaftliche Einstellungen konzipieren und in ihrer Untersuchung eine Akzeptabilität des neuen Reisepasses dort vermuten, wo sich erfolgreiche Begründungen für eine erhöhte Sicherheitsnotwendigkeit entlang von Themen wie illegaler Migration, Terrorismus oder aber Sozialbetrug etablieren.

Akzeptanz als den „erwarteten Nettonutzen" (z.B. Lüdemann/Schlepper 2013: 152) oder die „Willingness to Pay for Security" (diess. 2010) zu konzeptualisieren, das heißt derartige Oppositionen in Kosten-Nutzen-Rechnungen aufzulösen, bedeutet, Akzeptanz dann als gegeben

[39] So wurde in der Studie von Lüdemann und Schlepper (2013: 158) das Vorwissen über die einzelnen Maßnahmen erfragt. Alle Interviewten erhielten in der Studie hierzu gleichlautende Informationen.

anzunehmen, wenn die Beeinträchtigungen vom Nutzen der Maßnahme überwogen werden. Mit der Ausgangsannahme, dass die Bewertung der Technologie, mithin ihre Akzeptanz, davon abhängt, welche Bedeutung sie für die Bürger resp. Nutzer besitzt, verbindet sich folglich die Idee, dass Technologien der Überwachung dann akzeptiert oder dann am ehesten toleriert werden, wenn mit der individuellen Datenpreisgabe Gegenleistungen verbunden sind (vgl. hierzu auch Marx/Muschert 2007). Akzeptanz ist danach eine Abwägung von sich mit der Technologie verbindenden Vor- und Nachteilen, wie sie sich in der Akzeptanzforschung unter anderem hinter der Terminologie des „relativen Vorteils“ (vgl. z.B. Rogers 2003) bzw., und in Bezug auf den gesamten Adoptionsprozess, des sogenannten „Price of Convenience Model“ (Ng-Kruelle 2006: 15ff.) verbirgt. Die der Technologie zugeschriebenen Potentiale erweisen sich dabei als zentrale Elemente der Untersuchungen. Diese Attribute der Technologie werden entweder direkt ermittelt und erfragt und/oder gelangen indirekt über Kausalitätsannahmen in die Bestimmung der Akzeptanz – wie bei Weber (2008) ein erhöhter Komfort (Einfachheit), Bedienfreundlichkeit und ein erhöhtes Sicherheitsniveau oder ein erwartetes erhöhtes Sicherheitsgefühl (vgl. Lüdemann/Schlepper 2013, Pietsch/Fiebig 2012). Als prospektive Faktoren der Akzeptanz identifiziert dann etwa Weber (2008: 150) einen Zugewinn an Komfort durch das Fingerabdruckverfahren, also eine vergleichsweise „einfachere“, „bequemere“ oder „komfortablere“ Authentifizierung (vgl. auch Al-Harby et al. 2010). Dies mag wenig überraschen, ist die Wahrnehmung von Nützlichkeiten doch bereits Bestandteil der zugrunde gelegten Akzeptanzmodelle.

Letztlich wenden Lüdemann und Schlepper (2011: 133) jedoch ein, dass sowohl die Tatsache, wonach viele der Befragten in ihrer Untersuchung angeben, Abwehr- bzw. Schutzmaßnahmen gegen Kontroll- und Überwachungstechnologien zu ergreifen, ebenso wie die beobachtbare Etablierung von Protestveranstaltungen wie etwa „Freiheit gegen Angst“ auf ein Konfliktpotential statt Akzeptanz als ausdrücklicher Annahme der Bürger deutet (2013: 158f.). Hierin zeigt sich wiederum das modernisierungstheoretische Verständnis der Akzeptanz: (Erst) in öffentlichem oder wahrnehmbarem Protest offenbart sich Nicht-Akzeptanz. Es lässt sich aber auch als Indiz dafür lesen, dass in einer Gesellschaft nicht nur Entscheidungen problematisiert werden, sondern auch, dass Betroffenheiten nicht gleichsam hingenommen, geduldet und insofern ‚akzeptiert‘ werden.

1.3 Akzeptanz beforschen

Die Besonderheit der Fingerabdrucktechnologie lässt sich, wie zu Beginn skizziert, zum einen, darin sehen, dass sie unmittelbar auf den Körper gerichtet ist. Zum anderen ist es das Ziel von auf biometrischen Merkmalen basierenden Erkennungssystemen anhand etwa eines Fingerabdruckes automatisch, das heißt auf der Basis digitaler Datenverarbeitung, einzelne Personen zum Beispiel zu Zwecken der Zugangserleichterung oder -kontrolle zu identifizieren und/oder zu authentifizieren. Die Etablierung digitaler Fingerabdruckverfahren sowohl innerhalb staatlicher als auch alltäglicher Anwendungszusammenhänge ist, wie gezeigt (vgl. Kapitel 1.1), nicht nur Ergebnis technischer, sondern zugleich sozialer Innovationsprozesse. In diesen werden sowohl die konkreten Nutzungsformen als auch die Bedingungen ihrer jeweiligen Umsetzung ersonnen. Entlang nun dieser, sich an die Funktionalitäten der Technologie anschließenden, Versprechungen als auch der Kritik an diesen, entfaltet sich, so die Grundannahme der Akzeptanzforschung, der Rahmen innerhalb dessen sich (nicht) akzeptierendes Handeln verorten ließe. Dabei zielt die Forschung sowohl zur individuellen als auch gesellschaftlichen Akzeptanz der Biometrie darauf ab, Akzeptanz über objektivierbare Risiken zu bestimmen, um so die Grenzen der Zumutbarkeit neuer Technologien der Sicherheit und Kontrolle empirisch auszuloten. Diese Tradition der Akzeptanzforschung, wie sie sich auch in den empirischen Studien zur Akzeptanz niederschlägt, soll nachfolgend einer Kritik unterzogen werden, bevor sich Überlegungen daran anschließen, wie das amorphe Konzept Akzeptanz in einer Studie, die ihre Bedingungen erst sucht, handhabbar gemacht werden kann.

1.3.1 Kritisches zur Akzeptanz(-forschung)

Die mit der mittlerweile starken disziplinären Differenzierung (vgl. z.B. Petermann/Scherz 2005) angedeutete Unübersichtlichkeit vermag nicht darüber hinwegzutäuschen, dass sich Akzeptanzforschung vielfach durch eine gemeinsame Zielrichtung auszeichnet, die dadurch gekennzeichnet ist, dass sie im Wesentlichen darauf zielt, die Bedingungen für Akzeptanz, unabhängig davon ob es sich um ausdrückliche Zustimmung oder stillschweigende Anerkennung, Bestätigung oder Hinnahme handelt – Begrifflichkeiten, die sämtlich im semantischen Bedeutungsumfeld der Akzeptanz liegen (Lucke 1995: 74ff.) –, nicht nur zu ermitteln, sondern eine so verstandene Akzeptanz gleichsam zu erhöhen. So verbirgt sich hinter der modernisierungstheoretischen Einsicht eines gesellschaftlichen Minimalkonsenses eine Orientierung der Akzeptanzforschung an der Verfügung von Akzeptanz – gilt es doch zunehmend als

schwierig Zustimmung zu erhalten, mithin Akzeptanz für Entscheidungen zu erzeugen (Lucke 1998). Als „zeitgenössischer Schlüsselbegriff“ (Lucke 1995: 37) scheint die Frage nach der Akzeptanz insofern perspektivisch vereinnahmt.

1.3.1.1 Eine Kritik an ihrer konsensuellen Orientierung

Die in Kapitel 1.2.2 zugrunde gelegte Unterscheidung von individueller und gesellschaftlicher Akzeptanz verläuft nicht nur analog zu den von Ortwin Renn (1986: 45) differenzierten „Funktionen“ der Akzeptanz. Sie ist, worauf der Begriff der Funktion (ob nun in dieser Form intendiert oder nicht) hinweist, nicht nur an der Technologie*art* orientiert, welche jeweils im Hinblick auf ihre Annahme in Frage steht. Mit diesen Funktionen sind auch jeweils unterschiedliche Akzeptanz*akteure* befasst, welche wiederum häufig selbst eine ‚Akzeptanzfunktion‘ erfüllen. Der Begriff der ‚Akzeptanzfunktion‘ verweist auf die eingangs erwähnte modernisierungstheoretische Prämisse der Akzeptanzforschung. Indem sie als die „praktisch bedeutsamste Funktion des Partizipationsrechts“ gilt (Haug 2014: 236), führt sie gleichsam zurück auf den Begriff der Legitimation (etwa durch Verfahren, vgl. Luhmann 1969), der allerdings von faktischer Akzeptanz abstrahiert. Bereits seit den 1970er Jahren vollzieht sich auf der politisch-institutionellen Ebene eine solche Hinwendung zur „Beschaffung“ von Akzeptanz (Hennen 1994: 1, Gloede/Hennen 2005: 5, Ehrenberg-Silies et al. 2012: 2) und so liest sich der Begriff der „Akzeptanzkrise“, der – auch als Synonym für die „Zustimmungskrise“ –, anstelle der „Akzeptanz“ nicht selten in soziologischen Handbüchern zu finden ist (z.B. Hillmann 2007: 16 oder Reinhold et al. 2001: 11), als ein eindrücklicher Hinweis auf eine ebensolche Orientierung auch in der Wissenschaft. Nach Hillmann (2007: 16) bezeichnet er

> „die Erscheinung, dass zunehmend mehr Angehörige der modernen Industriegesellschaft aufgrund gesteigerter Sensibilität gegenüber möglichen negativen Auswirkungen der weiteren technisch-wirtschaftlichen Entwicklung die Verwirklichung großtechnologischer Projekte, z.B. Atomkraftwerke, chemische Großbetriebe und Verkehrsanlagen ablehnen.“

Wie etwa Gloede und Hennen (2005) zeigen, stellt sich das Fehlen von Akzeptanz im politischen Kontext von Anbeginn im Wesentlichen als eine Frage der Sicherung der Wettbewerbsfähigkeit und des Standorts der deutschen Wirtschaft dar – eine Problemwahrnehmung, wie sie sich in Schlagworten etwa des „skeptischen Meinungsklimas“, des „militanten Protests“, der „Kaufunlust“, der „Nutzungshemmnisse“ oder eines „geringen Diffusionstempos“ (mit weiteren Beispielen für politische Deutungen einer Akzeptanzkrise Petermann/Scherz 2005: 46, Jaufmann 1999: 207) andeuten. Um zu klären, wie wirtschaftliche Interessen befriedigt

und dennoch eine positive Aufnahme von Technologieentwicklungen befördert werden können (Gloede/Hennen 2005) ist die ‚Beschaffung' von Akzeptanz seit den 1970er Jahren bereits Bestandteil von Bundesforschungsberichten (Hennen 1994: 1), sowie die wissenschaftliche Auseinandersetzung mit ihren Voraussetzungen seit Mitte der 1980er Jahre „offizieller Gegenstand der Technologiepolitik" (Gloede/Hennen 2005: 5). Es entwickelt sich vor diesem Hintergrund nicht nur das Konzept der Technikfolgenforschung und -abschätzung (TA). Auf institutioneller Ebene vollzieht sich die Hinwendung zur Akzeptanzproblematik mit dem Antrag zur Einrichtung eines „Amts zur Bewertung technologischer Folgen beim Bundestag" 1973 durch die damalige Opposition (CDU), der sich nach „intensiver Auseinandersetzung" 1989 die Gründung des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) anschließt (Ehrenberg-Silies et al. 2012: 2). Dabei erscheint auch der Wandel der TA gleichsam institutionell angelegt: So wurden bereits im Memorandum des Bundesministeriums für Forschung und Technologie von 1989, als einer wesentlichen Etappe auf dem Weg zu ihrer Institutionalisierung, zwei wesentliche Typen der Technikfolgenabschätzung skizziert: eine an Techniklösungen orientierte und eine Richtung, die sich auf gegenwärtige und prospektive Konflikte, die von Bürgern im Umgang mit Technik bzw. als Betroffenheit von dieser erlebt werden, einstellt (vgl. Petermann 1999).

Auch eine Reihe von Forschungsprojekten im Rahmen der Sicherheitsforschung kennzeichnet eine deutliche Anwendungsorientierung und folgt dabei offenbar einer pragmatisch-präskriptiven Prämisse, wie sie zum Beispiel Würtenberger und Tanneberger (2010: 223f.) für die Aufgabe der Sicherheitsforschung folgendermaßen formulieren: Gilt die *erfolgreiche* Durchsetzung neuer Sicherheitstechnologien an die gesellschaftliche Akzeptanz gebunden, dann sei ihre Aufgabe darin zu sehen, dass die „angewandte Sicherheitsforschung, die in marktfähige Produkte münden soll, […] nur insoweit sinnvoll [ist], als die neuen Sicherheitstechnologien auf gesellschaftliche Akzeptanz stoßen." Zu diesen vielfach interdisziplinär angelegten Projekten, die unter dem Fokus der Akzeptanzgewährleistung die Implementierung neuer Technologien der Sicherheit und Kontrolle begleiten, zählt etwa das vom BMBF geförderte Projekt „Social-Area Framework for Early Security Triggers at Airports" (SAFEST, Baccelli et al. 2012), das sich der Herstellung von Akzeptanzbedingungen innovativer elektronischer Sicherheitssysteme im Flughafenbereich widmet und zu diesem Zweck die Akzeptanz von Sicherheitsmaßnahmen am Flughafen erhebt. Auch dem sozialpsychologischen Teilvorhaben MuViT-SozPsy „Exposition und Akzeptanz – Sozialpsychologische Studien in Re-

aktion auf Mustererkennung und Video Tracking“[40] liegt eine vergleichbare Zielrichtung zugrunde. Untersucht wird etwa der Einfluss des öffentlichen Diskurses auf die Einstellungen zu Chancen und Risiken sowohl der klassischen als auch einer geplanten automatisierten Videoüberwachung (Strack/Markel 2013: 10f., 26ff.), um daraus Kriterien von Akzeptanz forcierenden Informationen abzuleiten. So ist den Autoren zufolge „Akzeptanz nur dann interessant […], wenn sie informiert stattfindet“ (ebd.: 27). Sollen folglich die Grenzen des Akzeptablen ausgelotet werden, reduziert sich Akzeptanz hier auf eine ‚informierte Zustimmung‘. Als Einsicht in die vernunftgeprägte Rechtfertigung rückt der Begriff der Akzeptanz so jedoch erneut in die Nähe der Legitimation. Richtet sich eine zentrale Kritik an der Akzeptanzforschung also konkret darauf, dass diese von ihrer Beschaffung vereinnahmt ist (vgl. Gloede/Hennen 2005: 5f.), dann auch deshalb, weil sie weniger danach fragt, wie (nicht) akzeptiert wird, sondern, dass sie darauf zielt, „Akzeptanzfähigkeit“ (Hubig 2011: 156) herzustellen, das heißt, sich vor allem der „Wahrung der Bedingungen für Akzeptanz oder Nichtakzeptanz“ (ebd.) zuwendet. Mit einer solch praktisch-normativen Orientierung wird die an gesellschaftlicher Akzeptanz orientierte Forschung zugleich zum aktiven Akteur von „Akzeptanzpolitik“ (Barben 2010a, 2010b).

Gleichwohl entfaltet sich eine so verstandene kurativ inspirierte Prämisse der mit Akzeptanz befassten Forschung zu Sicherheits- und Kontrolltechnologien aber nicht ausschließlich in reinen, etwa ökonomischen, Verwertungskategorien. Die Strategien der empirischen Forschung liegen vielmehr zwischen Normativität, Reflexivität und Anwendungsbezogenheit. An Fragen der Ethik ausgerichtete Forschungsprojekte beschäftigen sich auf einer eher normativ-reflexiven Ebene auch kritisch mit den Zielsetzungen und Folgen von Sicherheitsmaßnahmen (z.B. das Projekt „Körperscanner: Reflexion der Ethik auf Technik und Anwendungskontexte“ [KRETA], zur Sicherheitsethik vgl. Ammicht-Quinn 2014, auch das Projekt MuViT ist an ethischen Fragen orientiert). Allerdings weniger auf die Bedingungen von Akzeptanz zielen auch sie eher auf eine, mitunter ethisch fundierte, Rechtfertigung, mithin die Akzeptabilität der in Frage stehenden Technologien, indem sie etwa den Wert der Sicherheit selbst befragen.

[40] Das Vorhaben ist Teil des vom BMBF geförderten Gesamtprojekts „Mustererkennung und Video Tracking: Sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen [MuViT] mit einer Projektlaufzeit Mai 2010 bis April 2013. Das Teilprojekt verfolgt mit seinem experimentellen Ansatz das Ziel „die Auswirkungen der neuen Technik der Mustererkennung auf die Wahrnehmung, das Erleben und das Sozialverhalten der Beobachtenden zu erforschen“ um daraus Faktoren abzuleiten, „die bei der Akzeptanz des neuen Systems entscheidend sind.“ (Strack/Markel 2013: 6)

1.3.1.2 Eine Kritik am normativen Impetus

Mit der Orientierung an Akzeptabilität tendieren Akzeptanzfragen dazu, zum Synonym für „Sozialverträglichkeit“ zu werden (Lucke 1995: 46f.). Damit riskiert die Forschung diese auf Bedingungen gesellschaftlicher Zumutbarkeit zu reduzieren. Und zumutbar ist dann ein Zustand, in dem sich die Technologien in ihrem Gebrauch oder auch nur Vorhandensein möglichst konfliktfrei in den Alltag einfügen und von den Nutzern bzw. Betroffenen an- oder zumindest hingenommen werden. Verlangt der in dieser Form verwendete Begriff der Akzeptanz nicht die Unterstellung einer Gleichsinnigkeit individueller Meinungen zu einem Sinnvorschlag (Luhmann 1969: 32f.), so ist es dann für die soziale Konstruktion von Akzeptanz auch nicht notwendig, dass Konsens und Verständigung tatsächlich stattfinden. In anderen Worten scheint die Orientierung der Akzeptanzforschung am öffentlich wahrnehmbaren Konflikt, die die Genese der Akzeptanz als soziologischen Schlüsselbegriff konturiert, ein Verständnis von Akzeptanz zu befördern, in dem für die akzeptierte Vermutung über Akzeptanz bereits das Ausbleiben von Widerspruch genügt (ebd.). Entspricht dies auch einer systemtheoretischen Perspektive auf das Akzeptanzphänomen als sozialem Sachverhalt und in diesem Zusammenhang als eine Form der Kommunikation (vgl. Luhmann 1984: 203ff.), dann umfasst Akzeptanz alle Fälle, in denen eine Kommunikation bejaht, das heißt angenommen wird, und dies unabhängig davon, was mit dem Sinnvorschlag verbunden wird – ist dies doch für eine erfolgreiche Kommunikation zunächst irrelevant (ausführlich dazu vgl. Kneer 2000). Die einer „prozeduralen Rationalität“ folgende Akzeptanzforschung produziert und reproduziert so ein Konzept der Akzeptanz als einer Einverständnisfiktion (vgl. Lucke 1995: 228f., 408f., vgl. Luhmann 1969: 32f.), insofern einer akzeptierten Annahme über die Akzeptanz, in der Widersprüche ebenso geglättet werden, wie die sie konstituierenden Bedingungen selbst unberücksichtigt bleiben.

Qualifiziert sich der systemtheoretische Ansatz von Akzeptanz für Georg Kneer (2000: 101) gerade dadurch, weil mit ihm normative Elemente, die sich auf die mit einer Zustimmungskommunikation verbindenden subjektiven Sinninhalte beziehen, von vornherein ausgeklammert werden, dann ist gleichwohl wenig darüber ausgesagt, wie Akzeptanz oder Ablehnung gesellschaftlich bewertet werden (ebd.). Die Problematisierung der An- oder Hinnahme von Technologien als Ausdruck von Akzeptanz verweist insofern auf spezifische Akzeptanzerwartungen, mithin auf „Regeln von Akzeptanz und Nicht-Akzeptanz“ (Lucke 1995: 151). Variieren diese mit den jeweils verfügbaren Maßstäben des Akzeptierbaren (ebd.: 111ff.), an denen Akzeptanz als Handlungsergebnis – etwa die Nutzung biometrischer Technologien – gemes-

sen wird, dann kann Akzeptanz entlang von Akzeptierbarkeitsvermutungen (ebd.: 143) selbst begründungsbedürftig werden (ebd.: 101). Wenngleich der Akzeptanzbegriff für Lucke (ebd.: 99) selbst keine Norm impliziert, zeigt doch ihre Definition, dass gesellschaftliche Normen einen Rahmen für das zu Akzeptierende bilden. Ausgehend von einer ersten Beschreibung der Akzeptanz als der „Chance, für bestimmte Meinungen, Maßnahmen, Vorschläge und Entscheidungen bei einer identifizierbaren Personengruppe ausdrückliche oder stillschweigende Zustimmung zu finden und unter angebbaren Bedingungen aussichtsreich auf deren Einverständnis rechnen zu können“ führt sie ihre Definition (ebd.) weiter aus und konzeptualisiert Akzeptanz dann als gegeben,

> „wenn Mitglieder einer Gesellschaft sowohl hinsichtlich der Legitimität (eines Vorschlags, einer Meinung, einer Handlung) wie in den hierfür verlangten Begründungen, angeführten Argumenten und eingeholten Rechtfertigungen in hohem Maße übereinstimmen; dem Akzeptanzobjekt grundsätzlich affirmativ gegenüberstehen und diesem verstandsmäßig und emotional ‚zugeneigt‘ sind; diesbezüglichen Vorschlägen, Argumenten und Maßnahmen auch im Konkreten uneingeschränkt zustimmen und diese ‚nach bestem Wissen und Gewissen‘ vorbehaltlos billigen und die betreffenden Personengruppen darüber hinaus bereit sind, das Akzeptierte notfalls auch gegen Vorschläge und ihm widersprechende Argumente zu verteidigen. Dies kann argumentativ oder in einer anderen, hierfür geeigneten bzw. für geeignet gehaltenen verbalen oder handlungsmäßigen Form geschehen und bezieht sich auch auf die Verteidigung des Akzeptierten gegenüber Mindermeinungen, Handlungsalternativen und biographischen Optionen.“

Für eine Erwartbarkeit von Akzeptanz erweisen sich folglich Werte und Normen, ein „Minimalkonsens an historisch gewachsenen und kulturell überlieferten Vorstellungen“ (ebd.: 149) als zentraler Bewertungsmaßstab der Akzeptanz, der im Begriff der Akzeptabilität seine Entsprechung gefunden hat. Macht Lucke hier also (indirekt) auf die Rolle von Akzeptanzdiskursen aufmerksam, die die Akzeptabilität und die Bedingungen von Akzeptanz selber konturieren, dann bedeutet dies, dass „soziologisch gesehen […] der Vorgang des Akzeptierens nicht ohne Anregung oder Anstoß von außen oder aus jedem gesellschaftlich-historischen Kontext losgelöst vollzogen“ wird (ebd.: 98). Akzeptanzdiskurse schaffen Argumentationsvoraussetzungen. In ihnen wird umrissen, woran Kritik zu üben ist, wovon man sich bedroht fühlen darf und zugleich, was einem nicht aufzufallen braucht (ebd.: 152):

> „Über Regeln der Akzeptanz und Nicht-Akzeptanz normiert wird [sic], worüber man sich aufregen *darf* und als ‚anständiger Bürger‘ seiner Entrüstung möglicherweise sogar Ausdruck verleihen *muss*. Sie umschreiben Vorfälle und Handlungen, deretwegen man sein Gesicht verliert und in Ungnade fällt. Umgekehrt definieren sie, wozu man sich in aller Öffentlichkeit bekennen kann und die Legitimitätsvermutung relevanter anderer dabei auf seiner Seite hat, und sie legen diejenigen Fälle fest, in denen man, wenn schon nicht die öffentliche Zustimmung aller zurecht vermuten, so doch die insgeheime Billigung vieler aussichtreich unterstellen kann.“ (ebd.: 151f., Herv. i.O.)

Ein Beispiel aus dem medialen Diskurs vermag diesen wichtigen Aspekt für das Verständnis von Akzeptanz noch einmal zu verdeutlichen: Am 31. Juli 2003 titelte die Zeit „Der Bürger wird rundum überwacht und findet nichts dabei“. Der Autor (Richard Herzinger) formulierte unter dieser Überschrift sein Unbehagen über eine Gegenwart, in der sich die Bürger scheinbar widerstandslos einem Sicherheits- und Bequemlichkeitsdiktat neuer, mit digitalen Daten operierender und zunehmend den bürgerlichen Alltag erobernder, Technologien fügen und sich damit regelmäßig nicht nur erweiterten Kontrollbefugnissen unterwürfen, sondern gleichsam riskierten, individuelle und gesellschaftlich verbürgte Autonomieansprüche einer „Gleichgültigkeits-Freiheit“ (ebd.) zu opfern – sei es durch die Gewöhnung an eine Allgegenwart der Videoüberwachung, die permanente Nutzung des Mobiltelefons oder die Speicherung von biometrischen Daten in den persönlichen Ausweispapieren. Die „Konsensfiktion“ (Luhmann 1964: 68f.) – die faktische Nutzung – wird folglich mit Akzeptierbarkeitsvermutungen unterlegt und so mithin gewertet. In diesem Zusammenhang erscheint der Hinweis entscheidend, dass, auch wenn Akzeptanz zum Inventar der Zivilgesellschaft geworden ist – Lucke konstatiert mit Blick auf den Sprachgebrauch von Politikern, Wissenschaftlern und Journalisten eine „sprachlich wohl bestellte ‚Akzeptanzlandschaft‘“ (1995: 35), mithin einen „inflationären Gebrauch“ (ebd. 1996b: 223) –, sie ein spezifisches Moment in einem je gesellschaftlich-historischen Kontext darstellt (vgl. ebd. 1995: 98).

Mit diesen ersten Einsichten in die Relativität des Akzeptanzbegriffes ist für die vorliegende Untersuchung, die ihren Ausgangspunkt vom Unbehagen an der Nutzung biometrischer Technologien im Alltag nimmt, mehrerlei gewonnen: Sie begründen, erstens, eine kritische Beurteilung der Akzeptanzforschung im Allgemeinen und zur Biometrie als neuer Sicherheits- und Kontrolltechnologie im Besonderen. Der Blick auf die Akzeptanzdiskurse, in denen die Akzeptabilität der Nutzung von Fingerabdrucktechnologien verhandelt wird, ermöglicht es, zweitens, die Rahmenbedingungen der Akzeptanz als in Frage stehende Werte zu betrachten – werden doch in ihnen Vor- und Nachteile der Technologie ausgehandelt. Sie konturieren als Argumentationsvoraussetzungen, woran legitim Anstoß zu nehmen ist,[41] und woran nicht und finden ebenso Eingang in die empirischen Untersuchungen von Akzeptanz wie sie die Grundlage über das neue Unbehagen an der Technologieakzeptanz bilden.

So hat das Konzept der Akzeptanz, wie Lucke (ebd.) auf dem Weg ihrer genealogischen Spurensuche konstatiert, dann auch ein spezifisches Subjekt im Blickfeld, namentlich das

> „aufgeklärte, zu Problemlösung und Risikobeherrschung qua identifizierendem und kontingentem Denken befähigte und in seinen Handlungen zurechnungsfähige Individuum der

[41] Etwa die nicht legitime Misstrauenserklärung an die Bürger.

> bürgerlichen Gesellschaft der Neuzeit […] und seine eigenverantwortlichen Handlungen und selbstbestimmten Unterlassungen."

Wenn also der in einer Gesellschaft jeweils verfügbare „Akzeptabilitätskatalog" (ebd.: 151) das Erwartbare umreißt, dann gehört zu diesen Zentralwerten in der Auseinandersetzung mit der Akzeptanz von Technologien der Sicherheit und Überwachung in erster Linie jener der Privatheit: Er gilt – als Ausdruck und Bedingung der persönlichen Autonomie – selbst als ein Wert, als ein autonomer Schutzraum gegenüber staatlichen Eingriffen (vgl. Rössler 2001). Mit der Preisgabe persönlicher Informationen, also aus dem Bereich des Privaten in die Öffentlichkeit, wird nun ein Verfall individueller Rechtsansprüche auf Privatheit konstatiert. Haben doch mit dem sogenannten Volkszählungsurteil 1983 (BVerfGE 65, 1) die Bürger als politische Subjekte Eingang in die Datenschutz-Kontroverse gefunden, lautet daher die Frage, warum in diesem Sinne riskante Technologien offenbar dennoch ‚akzeptiert' werden, wenn sie Privatheit bedrohen und damit einer Entgrenzung von Öffentlichem und Privatem, wie sie im Hinblick auf den Wandel der Sicherheitskultur diskutiert wird (vgl. hierzu z.B. Vasilache 2012) Vorschub leisten. So wird dann auch von kritischer Seite häufig davon ausgegangen, dass die Möglichkeiten von Überwachung ermöglichenden Technologien im Bewusstsein der Nutzer verankert sind oder sein sollten (z.B. Siemoneit 2007) – was, so ließe sich entwenden, allerdings auch zu einem entsprechenden Technikverständnis nötigt, das bei anderer mittlerweile veralltäglichter und gebrauchter Technik, zum Beispiel dem Fernseher oder dem Auto, gleichwohl nur selten vorhanden ist. So entrüstet sich der ehemalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar (2010):

> „Dieser ‚digitale Exhibitionismus' ist verhängnisvoll, weil die Betroffenen Teile ihrer Persönlichkeit preisgeben, ohne über eine wirksame Kontrolle über die Weitergabe der Information zu verfügen. […] Notwendig ist daher auch eine Sensibilisierung jedes Einzelnen für den bewussten Umgang mit seinen persönlichen Daten. […] Das Recht auf den Schutz unserer persönlichen Daten muss aber immer wieder aktiv eingefordert werden. Datenschutz ist auch Selbstdatenschutz. Dazu müssen die Bürger ihre Rechte eigenverantwortlich und selbstbestimmt wahrnehmen."

Diese Einschätzung entspricht der in Kapitel 1.1.2 im kritischen Diskurs identifizierten Aufforderung zur vorsorglichen Datensparsamkeit der Bürger. In der Vorstellung von Akzeptanz zwischen explizitem Annehmen und öffentlichem Protest sowie dem (informierten) Infragestellen als zivilgesellschaftlicher Norm konturiert sich folglich das Akzeptanz*problem* und prägt dann auch die in Kapitel 1.2.3 in Augenschein genommenen Akzeptanzuntersuchungen. ‚Die' Privatheit, als Basis einer bürgerlichen Grundhaltung und eines gesellschaftlichen Freiheitsverständnisses, welche durch die seit dem 11. September 2001 geschaffenen erweiterten Befugnisse staatlicher Akteure in Frage zu stehen scheint (vgl. zur Sicherheit im Fluchtpunkt

von 9/11 Krasmann et al. 2014: 63ff.), fungiert nicht selten als Gradmesser der Akzeptanz einzelner Technologien.

Kommen nun in der Akzeptanzforschung Fragen danach, was jene konstituiert, in dem Maße normativ daher, wie bereits feststeht, dass die Gesellschaft bestimmte Technologien, etwa auf der Grundlage einer wirtschaftlichen Verwendungsorientierung oder eines zu erzielenden Wertekonsenses, (nicht) akzeptieren soll, dann lassen sich solcherart normative Bestimmungen auch in der kritischen Befasstheit mit Biometrie in den Surveillance Studies ausmachen. Sie nehmen, aus einer Makroperspektive und von einem machttheoretischen Standpunkt aus, die technische Logik der Biometrie – die Kodierung der Körper – im Hinblick auf gesellschaftliche Exklusionsprozesse und, vor dem Hintergrund einer allgemeinen Entwicklung neuer Informations- und Kommunikationstechniken, neue Qualitäten der Kontrolle in Augenschein (z.B. Aas 2011, 2006, Lyon 2007, insb. Kapitel 5, 2001, Alterman 2003). Ausgehend von einer vermeintlich einheitlichen Funktionslogik und vor dem Hintergrund unbefragter Funktionalität (kritisch dazu Cole 2008, Muller 2010, Murray 2007) wird die zunehmende Akzeptanz biometrischer Technologien, zum einen, als Antwort auf diskursiv produzierte Ängste und Unsicherheiten gedeutet und die zunehmende Nutzung der Technologie dann als ein Bedürfnis, sich etwa vor Menschen mit ungewisser Identität zu schützen (vgl. Aas 2006: 156). Richtet sich der Blick zudem auf die gesellschaftlichen Rahmenbedingungen, aus denen heraus Fragen nach Identifikation erwachsen und diesbezügliche Notwendigkeiten vermittelt werden, gilt die Akzeptanz, zum anderen, als Ausdruck eines Bedürfnisses zur Absicherung und Beschleunigung des Lebens:

> „We inhabit a technologically mediated world where disembedded, quick and unambiguous communication seems to be of primary importance […] In this context, biometric identification joins passwords, PIN codes and other tools for securing and speeding-up our electronically mediated lives (Aas, 2005). Therefore, as we saw from the examples above, biometric identification can in certain contexts also exemplify privilege, enabling access to secured areas, or enabling, for example, frequent travellers to become ‚members of the club' and avoid time-consuming security checks at airports and border." (ebd.: 150)

In dieser Perspektive wird die Akzeptanz der Technologie aber nicht nur auf erfolgreiche Verunsicherungsdiskurse, mithin die Versprechen ihrer Anbieter, reduziert, sondern Biometrie gleichsam als ein stabiles Objekt bzw. eine fixierte, mithin fixierbare Praxis betrachtet, deren Folgen festumrissen und vorhersehbar erscheinen und welche sie per se als unethisch klassifizieren – unabhängig vom Kontext ihrer Verwendung. Kritisch zu dieser Tendenz einer Reifizierung der Biometrie im Kontext ihrer Verortung, insbesondere in ethischer Hinsicht, merken etwa Martin und Whitley (2013: 55ff.) an, dass (biometrische) Technologien jedoch

keine passiven Elemente einer neutralen Umwelt bleiben, sondern immer auch verstrickt sind in komplexe Systeme, die unterschiedliche Anwendungskontexte bereitstellen, die sie ebenso zu verändern vermögen, wie auch umgekehrt (in diesem Sinne auch Marx 2003: 371, Ball 2009: 652). Und in Bezug auf die Einhegung des Körpers in maschinelle Identifikationsprozeduren argumentiert dann auch Ball (ebd.), dass „the reality of that lived body in relation to surveillance is a far more complex issue" und auch das Ausbleiben von Protest nicht per se mit einer Akzeptanz gleichzusetzen ist.

Wenn mit Doris Lucke (1995: 119) gesprochen, Akzeptanzwahrscheinlichkeiten variieren, weil auch das „empirische Korrelat des Akzeptanzbegriffs im Zeitverlauf wandelbar" ist (ebd.: 100), dann können sich auch Formen von Widerstand ändern (ebd.: 101). In den Surveillance Studies etwa wird darauf hingewiesen, dass es in Bezug auf Kontrollerfahrungen keinen einheitlichen, gar globalen Effekt infolge der Einführung von Überwachungstechnologien gibt (vgl. McCahill/Finn 2014): So sind, zum einen, unterschiedliche soziale Gruppen in ungleicher Art und Weise von verschiedenen Formen der Überwachung betroffen (ebd.: 1). Dies gilt nicht nur im Hinblick auf die sich in die Technologien einschreibenden Kategorisierungen (vgl. Aas 2011), sondern auch durch das den Subjekten jeweils zur Verfügung stehende Kapital (Bourdieu 1983), das heißt jenen gesellschaftlich ungleich verteilten und sozial verfügbaren Praktiken und Gütern, die Menschen nicht nur soziale Status verleihen, sondern sie auch mit variierenden Handlungskompetenzen ausstatten. Entlang dieser machen etwa McCahill und Finn (2014) unterschiedliche Formen aus, mit denen sich Bürger in einzelnen Feldern der Überwachung aktiv ins Verhältnis zu Kontrolltechnologien setzen. In diesem Zusammenhang entfalten sich unterschiedliche Betroffenheiten sowohl in Abhängigkeit von den jeweils installierten Systemen als auch im Hinblick auf vorhandenes Wissen im Umgang mit ihnen. Damit steht dann auch nicht allein die Überwachungserfahrung per se im Vordergrund, wie sie etwa Arslan Butt (2011) im Hinblick auf öffentliche Videoüberwachung untersucht hat, sondern in den Blick geraten damit auch die Bedeutungen und Logiken unterschiedlichster „Felder" der Überwachung (vgl. McCahill/Finn 2014: 5 für das Feld der Kriminalitätskontrolle). Mit der konkreten Ausgestaltung eines Überwachungssystems variiert, zweitens, die Möglichkeit der Manipulation (ebd.) sowie, drittens, die Benutzungserfahrung. Überwachung „is not just ubiquitous; it is also subtle, deep, unobtrusive and selective", betonen dann auch David Murakami Wood und C. William R. Webster (2009: 260).

1.3.1.3 Eine Kritik an den vermeintlich eindeutigen Konstellationen

Die Akzeptanzforschung zu neuen Technologien, wie etwa biometrischen Verfahren, kennzeichnet eine Grundlegung funktionaler Versprechen (z.B. Sicherheit oder Bequemlichkeit) bzw. ihre Kritik (z.B. Gefährdung der Privatsphäre durch potentielle Überwachung) als Basis der Akzeptanz. Dagegen ist zunächst einzuwenden, dass damit zunächst kaum mehr als spezifischen Diskurskontexten entstammende Zuschreibungen Eingang in die Studien finden, welche nicht nur, grundsätzliche oder unterschiedlichen Anwendungssettings entsprechende, Zweck-Mittel-Zusammenhänge offerieren. Sie legen den (potentiellen) Nutzern auch unterschiedliche Umgangsweisen mit der Technologie nahe – Zuschreibungen, welche ihren Gebrauch dann schlicht als berechtigt begründen beziehungsweise von vornherein delegitimieren. Dies zeigt sich konkret darin, dass sowohl die Forschung zur gesellschaftlichen Akzeptanz als auch die wirtschaftswissenschaftlich orientierten und primär mit quantitativen Methoden arbeitenden Studien die Akzeptanz vor allem im Zugriff auf die Einstellungen der Nutzer zu den ex ante bestimmten Merkmalen der infrage stehenden Technologien erheben.

Wenn Akzeptabilitätsdiskurse das theoretische Fundament der empirischen Forschung bilden, dann wird der Prozess des Akzeptierens praktisch auf eine quantifizierbare Auf-Rechnung reduziert. Der Idee einer (funktionalen) Eindeutigkeit der Technologie folgend, legen diese Rechnungen zugrunde, dass sich die Bedeutung der Technologien in den im Vorfeld antizipierten negativen und positiven Konsequenzen auflösen ließe. In den Untersuchungen wird nicht nur angenommen, dass Technologien eindeutig in ihrer Bedeutung sind, sondern Akzeptanz ist danach das Ergebnis letztlich expliziter bzw. explizierbarer Abwägungen eines weithin von individuellen Merkmalen und Präferenzen bestimmten rationalen Entscheidungsprozesses, wie sie etwa auch in der Theorie des überlegten Handelns („Theory of Reasoned Action“, Fishbein/Ajzen 1975) und in der Weiterentwicklung zur „Theorie des geplanten Handelns“ („Theory of Planned Behaviour“, Ajzen 1985) zum Ausdruck kommt (vgl. kritisch hierzu Lucke 1995: 394f.). Die im empirischen Zugriff vorgenommene Fokussierung auf Vorteile und Risiken, und letztlich auf Bedrohungsgefühle und/oder Sicherheitserwartungen, ermittelt jedoch weniger eine Akzeptanz im Sinne einer mehr oder weniger ausdrücklichen Zustimmung. Vielmehr stellt sie einen Zusammenhang her – etwa zwischen Sicherheitsbedürfnissen und -technologien – und letztere erscheinen dann wiederum als Mittel, um erstere zu befriedigen. Die zugrunde gelegten Abwägungsprozesse werden damit gleichsam zu Wertfragen, wie es sich exemplarisch in der Konzeption der Akzeptanz von Oldemeyer (1988: 34ff.) andeutet. In dieser Bestimmung hängt die Akzeptanz davon ab, inwiefern die Bürger die „po-

sitiven“ Werte, die Technik erfüllen soll (etwa Wohlstand, Sicherheit, Wirtschaftlichkeit, Macht, Schönheit) gegenüber „negativen“ Werten (wie Gefahren, Schädigungen, Nebenfolgen) einschätzen und miteinander in Ausgleich bringen. Für die in Kapitel 1.2.3 skizzierte, primär quantitativ operierende Akzeptanzforschung zu Fingerabdruckverfahren bedeutet die hier zugrundeliegende Annahme – dass Technologien eindeutig in ihrer Bedeutung seien und ihre Zwecke und Risiken scheinbar objektiv auf der Hand lägen –, aber auch, dass sie eine vermeintlich objektive Sinnhaftigkeit verstärkt, indem sie Bedeutungszuschreibungen bereits durch die Kontextualisierung eines Objektes in den Fragen zu Bewertungen und Einstellungsmessungen selbst vornimmt (vgl. Krasmann et al. 2014: 45ff., 101ff.). Fragen wie jene „Um die Menschen in Deutschland vor den Gefahren des Terrorismus zu schützen, werden verschiedene Maßnahmen erwogen. Sagen Sie mir bitte, ob Sie den folgenden Vorschlägen zur Terrorabwehr zustimmen oder ob Sie diese ablehnen“ (Pietsch/Fiebig 2011: 269) etablieren auf diese Weise kognitive Rahmungen und riskieren so, Unsicherheitswahrnehmungen gleichsam zu reproduzieren, festzuschreiben und mithin Artefakte zu produzieren: Bedrohungswahrnehmungen werden, in anderen Worten, damit nicht nur erfragt, sondern gleichsam hervorgebracht (zu einer solchen Kritik an Befragungen zur Sicherheit- und Risikowahrnehmung in der Bevölkerung vgl. Krasmann et al. 2014: 45ff.).

Dass sich Einschätzungen der Bürger und Wahrnehmungen von Sicherheit und Unsicherheit aber nicht zwangsläufig an den in Frage stehenden Technologien festmachen, deutet sich in den Ergebnissen einiger Studien zur Akzeptanz neuer Sicherheits- und Kontrolltechnologien an. So zeigen sowohl Schlepper et al. (2015) als auch Bonß und Wagner (2012), dass unterschiedliche Sozial- und Kontrollräume mit ungleichen Wahrnehmungen von Sicherheit bzw. Unsicherheit verbunden sein können. Die in den Studien erfragte Bedrohungswahrnehmung und das Sicherheitsempfinden knüpfen sich danach nicht zwangsläufig an die in den Untersuchungen in Frage stehenden Technologien, sondern vielmehr an davon gegebenenfalls unabhängige kulturelle und sozialräumliche Prägung von (Un-)Sicherheitswahrnehmungen. Die Analyse der im Rahmen des SIRA-Projektes durchgeführten qualitativen Interviews mit Flugpassagieren zeigt etwa, dass der Kontext „Fliegen“ in dem Maße als unsicher und das Risiko eines terroristischen Anschlags als wahrscheinlich wahrgenommen wird, wie das Fliegen selbst letztlich für den Menschen fremd und unheimlich bleibt (ebd.). In umgekehrter Perspektive gilt dies auch für die Befunde der Studie von Schlepper et al. (2015). Werden von den Interviewten Fähren als weniger unsicher als Flugzeuge empfunden, dann verbinden sich mit ihnen dennoch spezifische Unsicherheiten. So sind es dann klassische „safety“-Maßnahmen, das heißt traditionell im Schiffsbereich etablierte Maßnahmen der Betriebssi-

cherheit, die – analog zum Risiko widriger Wetterbedingungen – Einfluss auf das Sicherheitsempfinden haben. Die Relevanz kulturell sozialräumlicher Kontextuierungen legt dann auch die in der Studie von Bug und Wagner (2015) ermittelte Bewertung der „Zweckmäßigkeit" der Sicherheitsmaßnahmen am Flughafen nahe (wobei die Frage auf den Schutz vor terroristischen Anschlägen zielt). Berücksichtigt man die Bedingungen dieses Sozialraumes, in dem bereits vor 9/11 Fluggäste mit einer Vielzahl an installierten Sicherheitstechnologien konfrontiert waren, dann könnte dies für die Frage der Akzeptanz bedeuten, dass etwa sogenannte Vielflieger mit Maßnahmen der Flug- und Flughafensicherheit so sehr vertraut sind, dass diese keine besondere Aufmerksamkeit (mehr) erlangen und gleichsam als gegeben hingenommen werden.

1.3.2 Akzeptanz beforschen: Methodologische Überlegungen

Ist vorangehend eine Reihe von Einwänden beschrieben worden, die sich sowohl an das theoretische Konzept der Akzeptanz als auch ihre empirische Erfassung richten, lässt sich als eine grundsätzliche Kritik formulieren, dass der bisher hierhin skizzierte Zuschnitt der Forschung ein reduziertes Verständnis der Akzeptanz zugrunde legt. Vor allem im empirischen Zugriff wird sie zu einem „technischen" Begriff (vgl. Lucke 1995: 40), dem, und darin liegt die wesentliche Gefahr technischer Begriffe in der (sozial-)wissenschaftlichen Forschung, die Nähe zu seinem eigentlichen Gegenstand fehlt, sie ihm sogar fremd zu werden droht (Vester 2009: 21). Mit den nachfolgenden Einsichten in das Akzeptanzkonzept, das Doris Lucke 1995 mit ihrer Monografie vorgelegt hat, gilt es Zugänge zur Akzeptanz zu identifizieren, ohne dabei jedoch den Untersuchungsgegenstand selbst zu präformieren. Akzeptanz ist, so zeigt ihre Typisierung (ebd.: 80f., Herv. i.O.), auf einer handlungstheoretischen Ebene mehrdeutig. Ihrer Bestimmung nach lässt sich diese, erstens, als „*Handlungsvoraussetzung* im Sinne einer Möglichkeitsbestimmung von Interaktion, Kommunikation, Koordination und Kooperation" verstehen, zu der „die Kenntnis und Anerkenntnis von Interaktionsregeln, als auch die Anerkennung des Interaktionspartners als einen in der Anwendung und Befolgung dieser Regeln erprobten und dementsprechend kompetent Handelnden" gehören. Sie kann, zweitens, eine „*Handlungsstrategie* im Sinne einer Zielerreichung sein", die strategisch eingesetzt wird, um damit etwas Anderes zu erreichen, oder, drittes, ein „intendiertes *Handlungsziel*" darstellen, in dem Akzeptanz zum Selbstzweck gerät. Dass daraus, viertens, Akzeptanz als faktisches *Handlungsergebnis* auftreten kann, mag sowohl Konsequenz einer nicht intendierten Wirkung als auch, fünftens, eine „unbeabsichtigte *Handlungsfolge*" sein. Eine beobachtbare, Verhal-

tenskonformität zumindest signalisierende, Handlung, wie sie mit letzteren Modi der Akzeptanz angesprochen ist, findet jedoch nicht zwangsläufig eine Entsprechung auf der von Lucke der Handlungsebene gegenübergestellten Einstellungsebene (ebd. 82). Damit lässt sich Akzeptanz, so dann auch die grundlegende Annahme der vorliegenden Untersuchung, nicht aus den subjektiven Einstellungen der Betroffenen ableiten, noch geht eine beobachtbare Nutzung der Technologie zwangsläufig in ‚individuellen' Zielen des Akzeptierenden auf.

Im Hinblick auf die Zurechenbarkeit von Handlungen ist die Frage der Akzeptanz also eine danach, welche Motive sich den Handelnden unterstellen lassen (ebd.: 84), die, – und das ist der zentrale Rahmen von Luckes Akzeptanzkonzeption –, sich nur im Verhältnis eines Subjektes zu einem spezifischen Objekt innerhalb eines konkreten Kontextes eruieren lassen (ebd.: 88ff.). Akzeptanz ist daher „*konstruktivistisch, interaktionistisch* und *interpretativ",* mithin verstehend, zu konzeptualisieren (ebd.: 92, Herv. i.O.):

> „Anzugeben ist nicht nur, *was,* sondern *was von wem* innerhalb welcher Gesellschaft, in welcher Situation und zu welchem Zeitpunkt sowie aus welchen Gründen und Motiven akzeptiert (oder eben abgelehnt) wird." (ebd.: 90, Herv. i.O.)

Mit ihrer genealogischen Analyse des Begriffes grenzt sich Lucke so auch von Akzeptanzdefinitionen ab, die affirmative Haltungen gegenüber einem Akzeptanzobjekt als Indikator dafür ausweisen, dass etwa „eine Innovation nicht nur legal, sondern auch legitim ist" (Endruweit 2014: 15). Akzeptanz impliziert nämlich, anders als Legitimität, nicht die „Übernahme bindender Entscheidungen in die eigene Entscheidungsstruktur" (Luhmann 1969: 7f.), sondern zielt auf Fragen der individuellen Annahme oder Ablehnung. So ist, etwa aus einer systemtheoretischen Perspektive, mit der Beobachtung über die Annahme einer Kommunikation, noch nichts darüber ausgesagt, was mit dem Sinnvorschlag verbunden wird (ausführlich dazu Kneer 2000).

Auf der Ebene des Fremdverstehens führt die Frage nach den Motivstrukturen entlang der von Alfred Schütz (1972: 104) getroffenen Unterscheidung von Um-zu- und Weil-Motiv – besteht doch zwischen beobachtbaren Handlungen und den Deutungen durch die Akteure für den Beobachter eine Differenz, die sich erst im Zugang zum subjektiven Sinnzusammenhang erschließen lässt. Motivstrukturen sind, in anderen Worten, nicht objektiv bestimmbar, sondern sinnadäquat nur dadurch zu rekonstruieren, dass sich die Akteure dem Erlebten selbst reflexiv zuwenden. Schütz (ebd.: 115ff.) zufolge wird Handeln durch einen Entwurf bestimmt, der ihm zeitlich vorausgeht und in dem sich Absichten und Pläne, die sogenannten Um-zu-Motive, widerspiegeln und welche auf bestimmte Intentionen des Akteurs verweisen, die dieser mit dem Handeln umzusetzen sucht. Die Weil-Motive hingegen sind von präreflexiven

Gewohnheiten und Deutungen, bereits gemachten Erfahrungen und gelernten, von Mitmenschen übernommenen, Erfahrungen geleitet, welche in die letztlich durchgeführte Handlung eingeflossen sind (vgl. auch Schütz/Luckmann 2003). Das damit unterbreitete Angebot zum Handlungsverstehen, das auch von den sogenannten Praxistheorien in expliziter Abgrenzung von einem intentionalistischen Handlungsbegriff geteilt wird (vgl. z.B. Reckwitz 2003), lautet, statt von einem explizit regelgeleiteten Handeln auszugehen, die implizit bleibenden Wissensbestände zu berücksichtigen, also das selbstverständlich Vorausgesetzte und fraglos Gegebene, wie es sich vor dem Hintergrund eingelebter Gewohnheit und Routinen etabliert.

Auf einer weiteren Ebene ist in diesem Zusammenhang das Objekt, auf das sich das Handeln – zumindest aus der Beobachterperspektive – richtet, mithin sein Sinn, zu spezifizieren, denn Akzeptanz, so die weiteren Ausgangsüberlegungen, findet ihre Bedingungen kaum in einer vermeintlich selbsterklärenden und in gewisser Weise sich selbst reproduzierenden Bedeutung von Akzeptanzobjekten. Vielmehr, und so betont es auch Lucke (1995: 119f.), ist Akzeptanz „nur in vergleichsweise wenigen Fällen […] gegenständlich, thematisch oder personell vorentschieden und dadurch weitestgehend determiniert." Die Beurteilung dessen, welche Bedeutung Akzeptanzobjekte haben, mithin was diese ‚sind', kann Lucke (ebd.: 120) zufolge kaum objektiv bestimmt werden, sind diese doch „vielverwendbar" und damit auch „prinzipiell interpretationsoffen". So ist eine mutmaßlich objektive Bedeutung bereits immer das Ergebnis von Konstruktionsleistungen der an Technologieinnovationen Beteiligten (vgl. Felt/Wynne 2007). Dies zeigt sich bereits darin, dass es nicht nur eine ‚Vision' der Fingerabdrucktechnologie gibt. Vielmehr existieren – mitunter bereits bevor sie überhaupt dem gestaltenden Zugriff unterliegt – immer zahlreiche konkurrierende Ideen darüber, welchem Zweck eine Technologie dienen soll (vgl. Felt/Fochler 2009: 4, vgl. Kapitel 1.1). In anderen Worten: wird etwa dem Fingerabdruckverfahren als einer Schlüsseltechnologie das Potential zugeschrieben, auf unterschiedlichste ‚Problemlagen' zu reagieren, so wohnen der Technologie selbst diese Passgenauigkeiten jedoch nicht inne.

Bildet die, sich in der Zusammenschau der Diskurse widerspiegelnde und in Kapitel 1.1.2 skizzierte, Bedeutungsambivalenz der Fingerabdrucktechnologie zwar den Problemhintergrund für das Forschungsprojekt, aus dem heraus diese Arbeit entstanden ist, so sprechen folglich auch techniksoziologische Befunde gegen eine ex ante bestimmbare Bedeutung der Fingerabdrucktechnologie: Technologiebedeutungen sind aber nicht nur Folge von Prozessen diskursiver Zuschreibungs- und Aushandlungsprozesse, sondern auch Ergebnis materialer Bearbeitungen (vgl. Pinch/Bjiker 1984) und daher, wie der Ansatz der „Social Construction of Technology" betont, „interpretativ flexibel" (ebd.: 421). Dies gilt nicht nur im Hinblick auf

ihren theoretischen Entwurf und ihre praktische Konstruktion, sondern sie erhalten sich zudem diese Flexibilität. Denn folgt man den Einsichten der interpretativen Soziologie (vgl. Schütz 2004, Schütz/Luckmann 2003, Garfinkel 1967, Blumer 2004) ist der Sinn der Objekte trotz diskursiver Bedeutungszuschreibungen für die Nutzer keineswegs festgelegt, sondern das Ergebnis sozialer Aushandlungsprozesse, in anderen Worten, eine soziale Konstruktion, die durch die Bedeutung bestimmt wird, die ihr die Akteure zuschreiben. Der Einsicht des sogenannten Thomas-Theorems folgend, wonach Menschen aufgrund der Bedeutung handeln, die die Dinge für sie haben (Thomas/Thomas 1970: 114), formt sich die Bedeutung dieser Dinge folglich „from within" (Garfinkel 1967: viii), das heißt erst und immer wieder neu in sozialen Aushandlungsprozessen in einem spezifischen Setting.

Auf einer zunächst diskursiven oder Verhandlungsebene bedeutet dies, dass, ethnomethodologisch betrachtet, Äußerungen nicht ohne ihren situativen Kontext verstanden werden können. Was die Technologie ist oder auch welchen Zwecken sie dient, muss also – ausgehend von der Flexibilität unterschiedlicher Anwendungssettings – im Hinblick auf die dort jeweilig vorherrschenden situativen Bedingungen untersucht werden. Situationen lassen sich, mit Erving Goffman (1974, 1977), als „Rahmen" verstehen, die, als ein analytisches Instrument, zudem der Klärung „dessen [dienen], was in Interaktionen und Aktivitäten eigentlich vor sich geht." (Knoblauch 2000: 172) Situative Rahmen, auch im Sinne mehr oder weniger institutionalisierter sozialer Zusammenhänge, geben etwa vor, welche Mitteilungen oder Handlungen jeweils an einem ‚Ort' als passend beziehungsweise unpassend gelten können. Folglich sind Interaktionen damit regelbestimmt, allerdings nicht so sehr, dass sie nicht auch offen für Gestaltung blieben. Der Rahmen reguliert vielmehr (typische) Erwartungen und umschließt die Möglichkeit dessen, was typischerweise kommunizierbar oder im Handeln möglich ist, was in diesem Sinne erwartbar ist.

Für das Erfassen der konkreten Materialität einer Technologie bieten sich zahlreiche Interpretationsrahmen an, gleichwohl der Begriff des (technischen) Objektes ebenso wie jener des ‚Dings' keinesfalls einheitlich bestimmt ist (vgl. hierzu Roßler 2016: 19ff.). Kritisiert Roßler (ebd.: 21) den Objektbegriff für die techniksoziologische Befasstheit als zu anspruchslos, ist es gerade seine Relationalität, das heißt die „Erkenntnisbeziehung" die in der Subjekt-Objekt-Konstellation „mitschwingt", als das sich „Entgegenwerfende" (ebd.: 20f.), die es für die Akzeptanz qualifiziert, weil damit noch nicht gesagt ist, was genau dieses Objekt nun eigentlich darstellt (zur Vielfältigkeit der Akzeptanzobjekte vgl. Lucke 1995: 88f.). Soll dennoch auf, im weitesten Sinne, techniksoziologische Einsichten als erkenntnisleitende Annahmen zurückgegriffen werden, dann lässt sich als ihr gemeinsamer Bezugspunkt bestimmen, dass Technik –

sei es als konkretes, etwa haptisch erfahrbares, Artefakt oder als größere Maschinerie –, immer auch in soziale Beziehungen eingebunden und insofern technologisch mit Vorstellungen und Praktiken verknüpft ist: sei es die in materiale Technik eingehenden Konstruktionsprozesse bzw. die in einer Technologie selbst vereinigten Praktiken und Wissensbestände (vgl. Hetzel 2005: 289). Geht Lucke (1995: 89ff.) zwar von immanenten, kontextuell isolierbaren Eigenschaften eines Objektes aus, konzipiert sie für seine Akzeptanz, neben ihm zugeschriebenen Bedeutungen, auch die ihm angehefteten „Chiffren und Symbole und die (sub-)kulturell codierten Signale" als relevant. Dies korrespondiert mit Einschätzungen zur Technikbedeutung, wie sie etwa Bernward Joerges (1996) oder Karl Hörning (2001) vorgelegt haben. Danach kann Technik nicht nur als Instrument dienen, mit dem sich spezifische Zwecke verbinden, sondern sie ist selbst Repräsentant sozialer Bedeutungen. Hörning (ebd.: 49ff.) macht in diesem Zusammenhang auf unterschiedliche Handlungsorientierungen aufmerksam, die dem menschlichen Umgang mit Technik zugrunde liegen und betont die sich innerhalb kultureller Praktiken entfaltenden subjektiven Motivlagen und kreativen Prozesses der Technikaneignung – etwa die Möglichkeit durch Technik Handlungs- und eigene Kompetenzspielräume zu erweitern, aber auch ästhetische Momente ihres Gebrauchs.[42] Demgegenüber will Joerges (1996) Technik im Modus von Handlungsinstitutionalisierung etwa durch technische Normierung (ebd.: 126ff.) im Sinne „auf Dauer gestellte(r) Verhaltensanweisungen an Geräte mit Legitimationshintergrund" (ebd.: 133) verstanden wissen, die in Form von Handlungszwängen auf die Praktik der Technikverwendung zurückwirken. Mit dieser sachtheoretischen Perspektive (vgl. auch Linde 1982) ist auf die sich in Technik verborgene Komplexität verwiesen, die die Objektivierung von Handlungen durch Trivialisierung ermöglicht, und die auch konstitutiv für die Etablierung der Akzeptanzforschung ist, da sie im Hinblick auf Techniknutzung oder -betroffenheit die Differenz von „Handlungsfeldern" zwischen technikentwerfendem Experten und technikverwendendem Laien (vgl. Schulz-Schäfer 2000: 19) konzipiert. Die technische und gerätetechnische Normfindung und die Festlegung von Grenzwerten (vgl. Joerges 1996: 127ff.) bilden dann auch einen nicht unwesentlichen Aspekt in der datenschutzrechtlichen Diskussion, innerhalb derer die Relevanz von Biometrie verhandelt wird (vgl. z.B. Hornung 2005). In diesem Zusammenhang wird zudem die Frage nach der Normativität der Technik virulent (vgl. Roßler 2016: 129f.), wenn hier die einer Technologie inhä-

[42] Technische Artefakte sind „Träger für kollektive Wertvorstellungen, wirken selbst an kulturspezifischen Stilprägungen mit und befördern Weltbilder. Sie sind auch offen für neue Zwecksetzungen, liefern Optionen, können unterschiedlichen ‚Herren' (Absichten, Gebrauchserwartungen) dienen. Keinesfalls alles, was mit Hervorbringung, Verbreitung und Gebrauch von Technik zu tun hat, kann auf technisch-funktionale Nutzenerwartungen zurückgeführt werden. Gefallen am Material oder Design, Lust an Bewegung und Geschwindigkeit, Neugierde, Suche nach sozialer Anerkennung, aber auch Unsicherheit, Missfallen und Überdruss – all diese Freuden und Leiden sind mit der Alltagstechnik verbunden." (Hörning 2001: 44)

renten Handlungsprogramme zum Ausgangspunkt gemacht werden, wie sie auch mit der in der Surveillance Studies dominanten Lesart der funktionellen Logik der Biometrie verknüpft sind (vgl. z.B. Aas 2006). Werden, wie es die grundlegende Kritik formuliert, menschliche Handlungen durch technische Abläufe substituiert, bildet die normative Handlungsmacht, mithin die „Politik" von Artefakten als Zwangs- und Sanktionsapparate (vgl. Winner 1980) ihr Fundament.

Ausgeblendet bleiben mit einem solchen Blick „auf fest fixierte Technizität", so eine wesentliche Kritik am sachtechnischen Determinismus (Rammert 2007a: 29, vgl. auch Hörning 2001: 165ff.), allerdings die Möglichkeiten der eigensinnigen Aneignung von Technologie im Prozess ihrer Verwendung, wie sie für die Frage nach den Bedingungen von Akzeptanz relevant werden. Eine weitere Kritik formuliert dann auch Beck (1997: 210) an der sachtheoretischen ‚Dekontextuierung' und der Annahme einer Formalisierung von Handlungsoptionen. Als kontextuelle Bedingungen unterscheidet er demgegenüber (ebd.: 169) etwa Nutzungsbedingungen, die in Anwendungssettings durch etablierte „sozial-kulturelle Nutzungsanweisungen" vorliegen, von jenen „harten", das heißt materiellen Handlungsumgebungen, zu denen auch die technologischen Strukturen gehören, in die die Technologie eingefügt ist und die aufgrund der vom Objekt ausgehenden Potentiale (sogenannte ‚affordances') Anschlusshandlungen ermöglichen können. Mit dem Blick auf die kontextuelle Einbettung von Technologien werden diese also eher als „Mittler" begriffen. Im Konzept des verteilten Handelns (Rammert 2007a: 92ff., 2007b: 21ff., Rammert/Schulz-Schaeffer 2002: 13) sind an technischen Handlungen unterschiedliche Instanzen beteiligt und das Objekt wird in einem größeren „Geflecht ‚vermischter' Aktivitäten" als „mit-handelnd" konzipiert (Rammert 2007a: 92). Akzeptanzhandeln verweist dann sowohl auf Bedingungen, die sich aus Interaktionen zwischen menschlichen Akteuren („Interaktion") als auch aus dem Umgang mit Technik („Interaktivität") innerhalb eines Anwendungsbereiches ergeben (ebd.). Auch in der Akteur-Netzwerk-Theorie, zu deren bekanntesten Vertretern Bruno Latour, Madeleine Akrich und Michel Callon gehören, wird das sozio-technische Netzwerk aus sozialen Akteuren, materiellen Dingen und/oder diskursiven Konzepten zum Ausgangspunkt der Analyse und auch hier gerät Technik als „Mittler" (Latour 2010: 70, 2005: 153f.) in den Blick. Anders jedoch als bei Rammert wird hier die Differenz zwischen Subjekt und Technik aufgehoben und letzterer ein gleichwertiger Akteurstatus zugewiesen. Mit diesem Symmetrieprinzip verbindet sich im Feld der Akteur-Netzwerk-Theorie die Aufgabe, die sich aus der normativen Handlungsmacht der Dinge ergebenden Wechselwirkungen zwischen den „Aktanten" zu analysieren. Die der Technologie eingeschriebene Logik fungiere zwar wie ein, aus dem Theatervokabular ent-

lehntes, Skript (vgl. Akrich 1992, 1995), mit dem sich untersuchen lässt, wie sich Vorstellungen von Technikgestaltern hinsichtlich der Nutzung von Artefakten in deren Materialität einschreiben: „like a film script, technical objects define a framework of action together with the actors and the space in which they are supposed to act." (Akrich 1992: 208) Skripte werden aber nicht allein durch Designer ‚geschrieben', sondern von den Be-Nutzern immer auch ‚mit'- und ‚umgeschrieben':

> „we cannot be satisfied methodologically with the designer's or user's point of view alone. Instead we have to go back and forth continually between the designer and the user, between the designer's projected users and the real users, between the world inscribed in the object and the world described by its displacement." (ebd.: 209)

Für Fragen der Akzeptanz kann die Analyse der Bedeutung des in technischen Objekten eingeschriebenen Wissens (etwa auch als Handlungsermöglichung oder -begrenzung) für vermeintliche Selbstverständlichkeiten in Bezug auf den Umgang mit Fingerabdruckverfahren sensibilisieren. Gleichwohl würde eine von der Akteur-Netzwerk-Theorie inspirierte Netzwerkanalyse zugleich das in Frage stehende und damit zu akzeptierende Objekt, von dem (Handlungs-)Delegationen ausgehen, zu stark in den Mittelpunkt der Analyse rücken.

So stellen die bis hierher skizzierten Einsichten unterschiedliche Fokusse und insofern auch unterschiedliche Analyse- und Denk*richtungen* für das Erfassen von Akzeptanz im Verhältnis von *Subjekt – Objekt* und *Kontext* zur Verfügung. Von diesen ausgehend lässt sich ein komplexer Zusammenhang der Akzeptanz der Technologie eruieren: erstens im Hinblick auf die sie begleitenden Diskurse sowie, zweitens, als Aneignung innerhalb der Bedingungen einer gegebenen Praxis und konkreter Benutzungsmöglichkeiten. In diesem Zusammenhang bestimmen auch Praxistheorien das Handeln nicht aus vorgängigen Intentionen, sondern ausgehend von der Frage nach Geeignetheiten und Relevanzen innerhalb spezifischer Praktiken, die mitunter Aneignungswissen stillschweigend bereitstellen (vgl. Hörning 2001: 157ff., Hillebrandt 2015, Reckwitz 2003).

Betrachtet werden soll Akzeptanz daher als Aneignung eines Objektes innerhalb „sozio-technischer Konstellationen" (Rammert 2007a: 92, 1988: 174), das gleichwohl offen bleibt für Adaption – und dies nicht allein deshalb, weil sich das Artefakt auf der Ebene der konkreten Benutzung als widerspenstig erweisen kann (Rammert/Schulz-Schaeffer 2002: 12). So ist Rammert (1999: 7f.) zufolge „die" Technik, keine „Substanz" und kein „Stoff mit bestimmten Eigenschaften", sondern „ein erst in der ‚Performanz' realisiertes spezifisches Werkzeug für einen Zweck in einem konkreten Kontext." Wird die Wirklichkeit, hier die Bedeutung der Technologie, diesem Verständnis nach auch im Vollzug und lokal hervorgebracht, dann, so

eine weitere Annahme, immer auch weiter, etwa in der konkreten Auseinandersetzung mit der Technik im Verlauf ihrer Nutzung (vgl. Lucke 1995: 120). Mit Blick auf das Prozesshafte des Akzeptierens selbst hält die Akzeptanzforschung für diesen Zusammenhang die auf das Englische zurückgehende Unterscheidung von „adopt“ und „adapt“ bereit (ebd.: 74). Meint das „Adoptieren“ demnach etwas so anzunehmen, wie es von den Akteuren gemeint, gedacht, beabsichtigt, als real angenommen ist, – eine Perspektive, die der Zielsetzung der klassischen Akzeptanzforschung, die das Produkt verkaufen will, entspricht –, verweist der Begriff des „Adaptierens“ dagegen auf das Moment des sich Aneignens und der möglichen Veränderung. Realisiert sich zudem der Zweck einer Maßnahme mitunter erst im Vollzug, dann kann zu adaptieren auch das Einpassen in vorgegebene Strukturen wie auch die aktive Anpassung an eigene Zwecke bis hin zur Verfremdung bezeichnen (ebd.: 120, vgl. für diese ebenfalls von der kulturalistisch orientierten Technikforschung geteilte Einsicht z.B. Hörning 2001) und geriete dann auch unter dem Stichwort der Gewöhnung in den Blick.

2 Über die Studie zur Akzeptanz: Die Entwicklung der durchgeführten Arbeiten

Die vorliegende Untersuchung zielt darauf am Beispiel des digitalen Fingerabdruckverfahren die Akzeptanz neuer Kontrolltechnologien im Alltag zu untersuchen und Annahmen über ihre Bedingungen zu formulieren. Den Ausgangspunkt der Untersuchung bildet ein Verständnis von Akzeptanz als „Resultat sozialer Konstruktionen“ und Aushandlungsprozesse (Lucke 1998: 20). In Anlehnung an techniksoziologische Erkenntnisse werden Akzeptanzobjekte als „interpretativ flexibel“ (Pinch/Bjiker 1984: 419) und Formen ihrer Akzeptanz in subjektiven Aneignungsprozessen vermutet. Ein solches Verständnis der Akzeptanz steht genuin in der Tradition des verstehenden soziologischen Zugangs und interpretativen Paradigmas der Sozialforschung. Wird die Welt diesem zufolge von den Individuen nicht als gegeben vorgefunden, sondern erweist sie sich vielmehr als Ergebnis des interpretativen Umgangs mit Deutungsangeboten, dann waren dem empirischen Vorgehen folglich qualitative Verfahren angemessen, die auf das Verstehen des mit einem Handeln subjektiv gemeinten Sinns (vgl. Schütz 1972: 13) zielen. Die Prozesse der Bedeutungsherstellung und ihre Reflexion durch die Nutzer der Fingerabdrucktechnologie wurden deshalb in methodischer Triangulation (vgl. Flick 2011, 2005) mittels der Beobachtung von Registrierung- und Nutzungsprozessen und anschließenden thematisch strukturierten Interviews in unterschiedlichen Anwendungssettings erfasst.

Die Untersuchung setzte an einem Verständnis der Bedeutungsherstellung im Vorfeld der (Einstellungs-)Akzeptanz von Nutzern beziehungsweise im Prozess verhaltensbezogener Akzeptanz an. Erwartet wurde zunächst, dass die Be-Deutung und Wahrnehmung und insofern auch die Akzeptanz von Fingerabdrucktechnologien im Alltag vom jeweiligen Anwendungssetting und damit gleichermaßen von sozialen wie medialen Aushandlungsprozessen abhängig ist. In diesem Zusammenhang war es im Rahmen der Projektannahmen zunächst von besonderer Bedeutung, wie als wichtig erachtete diskursive Spannungsfelder *Gefährdungen vs. Schutz der Privatsphäre*, *Degradierung vs. Distinktionsgewinne* sowie *Überwachung vs. Sicherheit* von den Nutzern thematisiert und reflektiert werden, denn nur wenn diese Spannungsverhältnisse zumindest in der Wahrnehmung der Betroffenen austariert werden, könnten sich – so die Ausgangsthese – biometrische Kontrolltechniken tatsächlich als Alltagstechnologien außerhalb segmentärer Bereiche staatlichen Zwangs etablieren.

Diese These – ebenso wie theoretische Vorüberlegungen in der qualitativen Forschung generell – hatte gleichwohl nicht die Funktion, eine empirisch möglichst gehaltvolle Hypothese zu

generieren, sondern sie diente dazu, für bestimmte Aspekte zu sensibilisieren, die mit dem erforschten Gegenstand in einer inhaltlichen Beziehung stehen. Theoretische Vorannahmen rahmen den Erhebungsprozess und werden für die Interpretation herangezogen, können aber vor dem Hintergrund eines kontinuierlichen Vergleichs zwischen den erhobenen Daten und Interpretationsvorschlägen auch verworfen werden. Vor diesem Hintergrund und mit dem Ziel Erfahrungen, Handlungen und Wissen in Bezug auf die Nutzung der Technologie zu verstehen, ohne dabei den Begriff der Akzeptanz im Vorhinein allzu sehr zu präformieren, lässt sich das Vorgehen im Feld einer gegenstands-begründeten Theorie (Glaser/Strauss 1998, Strauss 2004, Strauss/Corbin 1996) verorten. Die Angemessenheit eines solchen Forschungsstils für das Forschungsprojekt lässt sich, zum einen, darin sehen, dass die Grounded Theory, vor allem in der Variante Anselm Strauss‘ (vgl. Strübing 2008: 37ff.)[43], in einer Theorietradition des Pragmatismus und des symbolischen Interaktionismus steht. Während im Pragmatismus davon ausgegangen wird, dass der Sinn, mit dem Personen ihre Handlungen versehen, im Handeln selbst gründet, verfolgt eine dem symbolischen Interaktionismus verbundene Forschungsstrategie das Ziel den subjektiven Sinn den Individuen mit ihren Handlungen und ihrer Umwelt verbinden zu rekonstruieren (vgl. Blumer 2004). Ein in den Interviews zu ermittelnder Sinn, als ein (Nach-)Denken der Befragten über die Technologie, steht folglich „nicht außerhalb der Wirklichkeit, sondern ist sowohl von deren praktischer Erfahrung geprägt als auch selbst konsequenzenträchtig.“ (Strübing 2008: 40) Die sowohl im Pragmatismus als auch im Symbolischen Interaktionismus zu findende Annahme einer einem ständigen Wandel unterworfenen Realität findet sich dann auch im Theoriebegriff der Grounded Theory wieder: „Weil Theorien nicht Entdeckungen (in) einer als immer schon gegebenen zu denkenden Realität, sondern beobachtergebundene Rekonstruktionen repräsentieren, bleiben auch sie der Prozessualität und Perspektivität der empirischen Welt unterworfen.“ (ebd.: 39) In forschungspragmatischer Hinsicht findet sich diese erkenntnistheoretische Position auch in einem Leitsatz der von Glaser und Strauss (1998: 15, Herv. i.O.) gemeinsam verfassten Einführung zur Grounded Theory wieder: „*Theorie zu generieren, ist ein Prozeß*“. Und so liegt die Eignung des Forschungsstils, zum anderen, darin, dass mit den nachfolgend beschriebenen Verfahren der subjektive Beitrag der Forschenden, der im Übrigen nicht erst mit der Formulierung von Thesen und Problemstellungen entsteht (vgl. Meinefeld 2005: 274), systematisch und nachvollziehbar in den Erkenntnisprozess eingebracht wird. Im Folgenden werden daher die einzelnen Schritte und Stadien der Erhebungen sowie die im Rahmen des als zirkulär verstandenen Forschungsprozesses, das heißt im Rahmen der Verflechtung von Erhebungs- und

[43] Zu den Unterschieden in den Weiterentwicklungen der Grounded-Theorie-Methodologie vgl. z.B. Strübing (2008: 65ff.).

Auswertungsphasen, notwendig gewordenen Modifikationen im Hinblick auf den Untersuchungsgegenstand beschrieben.

2.1 Eine ‚Ethnografie' der Akzeptanz

Ethnographie kann unabhängig ihrer verzweigten interdisziplinären Verortung als eine Forschungsstrategie, aber auch -haltung verstanden werden, die darauf zielt, gesellschaftliche Phänomene in der ihnen eigenen Komplexität und Ganzheit aus der Sichtweise der an ihnen beteiligten Akteure zu verstehen und zu beschreiben. Akzeptanz ethnographisch zu beforschen heißt dann sich in die natürlichen Settings zu begeben, in denen ein solches Handeln beobacht- und Nutzer zu diesem befragbar sind. In Abgrenzung zu einem konventionellen Verständnis der Ethnographie – die Einklammerung trägt in methodologischer Hinsicht der Kontroverse darüber, was als ‚echte' Ethnografie gelten darf (vgl. Knoblauch 2002), Rechnung – ist die vorliegende Arbeit angelehnt an ein Vorgehen einer demgegenüber „fokussierten Ethnologie" (Knoblauch 2001, 2002), da sie, einerseits, weniger auf die umfassende Darstellung eines Feldes als einem spezifischen Setting, als auf die, aus einer komparativen Perspektive (Knoblauch 2001: 137) heraus angelegte, Analyse bestimmter Handlungszusammenhänge, mithin auf „Handlungsprobleme der Beobachteten" (ebd.: 132) zielt. Vor diesem Hintergrund legt sie, andererseits, in stärkerem Maße theoriegeleitete Vorentscheidungen (ebd.: 133ff.) im Hinblick auf die Auswahl von zu beobachtenden Situationen als auch bei der Wahl der als rahmengebend angenommenen Settings zugrunde: Ermittelt werden sollen „particulars of situated performance as it occurs naturally in everyday social interaction." (Erickson 1988: 1083 zit. in Knoblauch 2001: 132) Lautete in diesem Zusammenhang die Vorannahme des Projektes, dass die Bedingungen von Akzeptanz sowohl in diskursiven und interaktiven Aushandlungsprozessen, zwischen Fingerabdruckgebern und -nehmern[44], sowie tatsächlichen Nutzungserfahrungen, das heißt der „medialen Interaktivität" (Rammert 2007b: 20) von Akteur und Technik zu suchen sind, dann war mit dem auf einen Vergleich angelegten Untersuchungsdesign ein längerer, in der Regel mehrmonatiger Aufenthalt im Feld – als Maßgabe einer hinreichenden Vertrautheit, wie sie etwa Hitzler und Gothe (2015: 10, vgl. auch Hitzler 2009: 211f.) als Kriterium ‚echter' Ethnographie formulieren –, von vornherein und nicht zuletzt auch aus forschungspragmatischen Gründen, nicht zu realisieren. Ausgehend von einer

[44] Als Fingerabdrucknehmer wird in diesem Zusammenhang jene Personengruppe bezeichnet, die im Rahmen von Registrierungsprozessen Fingerabdrücke erfasst (z.B. Kassierer, Behördenmitarbeiter), als auch jene Personen, die Einrichtungen leiten, in denen Fingerabdruckverfahren verwendet werden (z.B. Supermarktbetreiber, Videothekeninhaber).

eher allgemeinen Bestimmung der Ethnographie, als einer „flexible[n], methodenplurale[n], kontextbezogene[n] Strategie“ (Lüders 2005: 389), mit der auf verschiedenen Wegen Informationen gesammelt werden können, ist jedoch mit den in dem Projekt verwendeten Datenerhebungsmethoden zumindest ein Teil der methodischen ethnographischen Gütekriterien erfüllt. Aber nicht nur das: Im Hinblick auf die im Rahmen der vorliegenden Arbeit notwendig gewordenen Modifikationen (vgl. Kapitel 2.3) bewährte sich ein, gleichwohl nicht ausschließlich unter ethnographischen Gesichtspunkten, relevantes Prinzip der Befremdung der eigenen Perspektive, dass nämlich im Feld – der Akzeptanz der Fingerabdrucktechnologie – vielleicht nicht „alles“, aber doch vieles mehr „beachtenswert ist, weil man erst im Verlauf des Forschungsprozesses erkennen kann, was hier – aus den Relevanzsetzungen der Untersuchten heraus oder diese eben *explizit* konterkarierend – *besonders* beachtenswert, deutungs- und erklärungsbedürftig ist.“ (Hitzler 2009: 213, Herv. i. O.)

2.1.1 Die Auswahl der Untersuchungssettings

Ausgehend von der Vorannahme, dass sich in unterschiedlichen Anwendungssettings die Akzeptanz in Abhängigkeit von variierenden Aushandlungen und damit differierenden Sichtweisen auf die Technologie formt, resultierte daraus für das Sampling eine Strategie, die, indem sie die Untersuchungsfelder vorab festlegte, die wesentlichen Annahmen der Grounded Theory (zum theoretischen Sampling vgl. Glaser/Strauss 1998: 53) ebenso wie der klassischen Ethnographie (vgl. z.B. Hitzler/Gothe 2015: 12) modifiziert, da diese demgegenüber entweder am Stand bereits interpretierter Daten oder etwa den Dynamiken und Strukturen des Feldes ausrichtet ist. Weil zudem längst nicht von einer flächendeckenden Verbreitung der Technologie auszugehen war, orientierte sich die Auswahl der Untersuchungssettings zunächst an den faktisch gegebenen Anwendungen in Deutschland und so vorgefundenen, jeweils anzunehmenden variablen Zwecken und Funktionen der Fingerabdrucktechnologie, und damit auch an Untersuchungssettings, die sich in den Einführungslogiken resp. -rationalitäten, die zwischen Sicherheitspolitik, Kontrollbedarfen und ökonomischen Interessen changieren, unterscheiden.

Maßgeblich waren hierfür nicht allein spezifische Sachzusammenhänge, wie etwa die durch Fingerabdruckverfahren ermöglichte Zugangskontrolle oder ihr Einsatz als Bezahlverfahren, sondern vielmehr unterschiedliche ‚soziale Orte‘ (in Anlehnung an Bernfeld 1996) der Technologieanwendung (wie etwa *Supermarkt* oder *Behörde*), die sich mutmaßlich im Grad der Freiwilligkeit der Partizipation bei der Preisgabe biometrischer Merkmale unterscheiden. Be-

misst man Freiwilligkeit zudem an der effektiven Möglichkeit, ‚nein' sagen zu können (Ladwig 2006: 90 mit Bezug auf Cohen 1990, vgl. Hornung 2005: 379 zu „Ausweichmaßnahmen" im Hinblick die ‚faktische' Durchsetzungsebene, in diesem Sinne auch Marx z.B. 2006a), dann lagen der Auswahl auch institutionelle Vorgaben zugrunde, die zudem quer zu den einzelnen Anwendungsfeldern liegen. Während der Einsatz eines biometrischen Systems zur Zeiterfassung in einer *Arztpraxis* verpflichtend erfolgte, ist im behördlichen Setting die Preisgabe körperlicher Daten für den Personalausweis faktisch freiwillig, für die Ausstellung eines Reisepasses hingegeben obligatorisch. Auch in *Schulen* kann die Teilnahme an einem bargeldlosen Bezahlverfahren, das durch das Fingerabdruckverfahren realisiert wird, zur Wahrnehmung von Sozialvergünstigungen obligatorisch sein. Berücksichtigung fand in diesem Zusammenhang auch das Angebot funktionsgleicher Alternativen zum Fingerabdruckverfahren im jeweiligen Untersuchungssetting. Bei Bezahlverfahren in Schulen oder Supermärkten etwa kann, im Gegensatz zur Behörde, auf andere Möglichkeiten wie z.B. die Bar- oder Zahlung per EC-Karte zurückgegriffen werden. In Settings wie *Automatenvideotheken* stehen alternative Zugangsmechanismus unabhängig von einer Registrierung von Daten des Fingerabdrucks in der Regel nicht zur Verfügung. Gleichwohl lautet die These, dass der situative resp. interaktive Rahmen der Fingerabdruckerfassung bestimmend für die Wahrnehmung von Freiwilligkeit und Zwang ist.

2.1.2 Teilnehmende Beobachtungen

Im Rahmen der fokussierten Ethnographie wurden nach dem Prinzip „follow the people" (Marcus 1995: 106) innerhalb der ausgewählten Settings natürliche Situationen, das heißt Anmeldungen und Benutzungen der Technik, beobachtet, um die Relevanzen der Beobachteten zu erfassen (Knoblauch 2001: 134) und die Wissens- und Erfahrungsstrukturen der Beteiligten, die den Sinn ihrer Handlungen konstituieren, zu rekonstruieren. Die mehrtägigen teilnehmenden Beobachtungen von Registrierungs- und Nutzungsprozessen zielten folglich darauf, einen Zugang zur Situiertheit (vgl. Suchman 1985) eines beobachtbaren Nutzungshandelns zu erhalten. Dabei wurde eine teilnehmende, mal offen und mal (zumindest gegenüber den Fingerabdruckgebern) verdeckte, das heißt den Nutzern/Antragstellern zu Beginn der Beobachtungen nicht offen gelegte, beobachtende Forscherrolle eingenommen.

Dem Einsatz des Instruments der Beobachtung geht die Annahme voraus, dass durch die Teilnahme an „face-to-face-Interaktionen bzw. die unmittelbare Erfahrung von Situationen Aspekte des Handelns und Denkens beobachtbar werden, die in Gesprächen und Dokumenten

– gleich welcher Art – über diese Interaktionen bzw. Situationen nicht zugänglich wären." (Lüders 2001: 151) Soll die Bedeutungskonstitution empirisch, materialgestützt in natürlichen Gesprächssituationen als einer thematischen Aushandlung untersucht werden, dann liegt der Einsatz der Beobachtung von Interaktionen zugleich nahe, da nur mit ihr der Zugang zu diesen ermöglicht wird. Interaktionen sind daher als Situationen zu verstehen, in denen Bedeutungen nicht nur angewendet, sondern auch verändert werden. Eine auf den Beobachtungen basierende Interaktionsanalyse zielt folglich auf die detaillierte Beschreibung der beobachteten Gespräche, in anderen Worten, auf „die Untersuchung konkreter ‚Exemplare' von Interaktion in alltäglichen Settings" und legt den Fokus auf die „Wechselwirkung der Interaktionspartner [und] die Berücksichtigung des Kontextes" (Hornecker 2004: 2). Mit teilnehmender Beobachtung lässt sich also festhalten, was in bestimmten Momenten von Situationen ‚passiert' und sie kann, unter Bezugnahme auf die individuellen Sinnsetzungen der Akteure, dazu dienen, Handeln erklärend zu verstehen (zur den graduellen Abstufungen akzeptierender Verhaltensweisen vgl. Lucke 1995: 208ff.). Im Hinblick auf die Auswahl der Anwendungssettings wurde gleichsam vorausgesetzt, dass Aushandlungsprozesse als von Eigendynamiken gekennzeichnet betrachtet werden können, die in der Situation selbst zu verorten sind. In den Blick gerät somit nicht nur Sprache als gegebenenfalls korrektive Austauschhandlung, sondern auch nonverbales Verhalten als eine gemeinsame Performance sowie die Rolle der materiellen Umgebung. Eingang in die Protokolle, die je nach situativem Erfordernis teils während, teils im Anschluss an die Beobachtungen angefertigt wurden, fanden neben Gesprächsinhalten, als möglichst wortwörtliche Dokumentation des Gesprochenen, daher auch mimische, nonverbale Gesten, die sowohl im Gespräch als auch im direkten Umgang mit der Technik selbst beobachtet wurden. Dabei muss berücksichtigt werden, dass die handschriftlich angefertigten Protokolle – vermutet wurde, dass ein elektronisches Aufzeichnen der beobachteten Interaktionen mit einer hohen Ablehnungsquote seitens der Fingerabdrucknehmer und -geber einhergehen sowie deren Verhalten erheblich beeinflussen würde – immer schon Produkte eines „Transformationsprozesses" (Lüders 2005: 396), das heißt immer schon Reproduktionen von als wichtig erachteten Aspekten darstellen. Dasselbe gilt für Kontextbeschreibungen, die auf den während der Beobachtungen als typisch wahrgenommenen Abläufen und Bedingungen im Setting basieren. Um diese Subjektivität des Forschers zumindest zu reduzieren, erfolgte nicht nur eine möglichst sachliche Verschriftlichung des Beobachteten (vgl. Dellwing/Prus 2012: 172ff.), sondern in der Regel wurden die Beobachtungen innerhalb eines Settings durch zwei Forscher durchgeführt, um so auch Selektivitäten in der Wahrnehmung möglichst zu minimieren. Mit der Frage nach den Eigenheiten des Settings ist gleich-

wohl ein zweiter Einwand verbunden, in dem sich auch die wesentliche Kritik an der fokussierten Ethnographie herauskristallisiert. Danach realisiert sich die Möglichkeit zum Erkennen des Eigensinnigen erst durch eine Vertrautheit aufgrund längerer Feldaufenthalte (vgl. Hitzler 2009: 212ff.). Die Entgegnung Knoblauchs (2002: 130), dass sich anhand soziologischen Hintergrundwissens, mithin vorhandenen Kontextwissens, die Fremdheit des Feldes – die Akzeptanz in unterschiedlichen Settings – relativieren ließe, schaffte jedoch nur bedingt Abhilfe, da damit wiederum nur vermeintlich objektive Bedingungen (etwa die Frage der Akzeptabilität der Technologie) in den Fokus geraten wäre. Für ein Verstehen des Typischen des Settings wurden daher möglichst viele Interaktionen und Interaktivitäten beobachtet, sodass letztlich mehr Beobachtungen als nachträglich geführte Interviews vorlagen. Gleichwohl gingen nicht allen Interviews auch Beobachtungen von Registrierungs- und/oder Nutzungsprozessen unter Beteiligung der jeweils Befragten voraus (zu den Zugangsbedingungen in den jeweiligen Settings vgl. Kapitel 2.2), sodass in diesen Fällen auf der Basis der Beobachtungen als typisch verstandene Abläufe vorausgesetzt wurden. Für ein erweitertes Verständnis der jeweiligen „Sozio-Logik“ (Hirschauer/Amann 1997: 20 zit. in Dellwing/Prus 2012: 84) wurden zudem in den einzelnen Settings Fingerabdruckabnehmer als „Träger von Kontextwissen“ (Bogner/Menz 2005: 37) im Rahmen des Projektes befragt (eine Übersicht über die Interviews findet sich in Kapitel 2.2). Weil diese, mehr oder weniger, direkt in die praktische Tätigkeit der Fingerabdrucknahme innerhalb der Settings involviert sind oder „aufgrund der Nähe zu [dem] persönlichen Handlungsfeld zumindest genauere Kenntnisse“ besitzen (ebd.: 43), wurden damit aus der Perspektive dieser ‚Experten‘ erste Einsichten in und Informationen über Handlungsabläufe und organisationale Konstellationen innerhalb der jeweiligen Settings generiert. Ergänzend dazu wurden thematisch einschlägige Dokumente, die in bzw. zu den jeweiligen Settings vorlagen, gesammelt und inhaltsanalytisch ausgewertet.[45] Neben diesen Erkundungen der Setting-Realitäten wurde auch die eigene Person der Forscherin zum Werkzeug, indem das den im Projekt Beteiligten Fremde der Fingerabdruckabgabe immersiv, das heißt durch ein Eintauchen in die Lebenswirklichkeit der Untersuchten (vgl. Dellwing/Prus 2012: 53, 84), in unterschiedlichen Settings durch Registrierungen der Fingerabdruckdaten vertraut gemacht wurde: Exemplarisch wurde so am eigenen Leib erfahrbar, was es bedeutet, bei der Beantragung des Reisepasses zur Fingerabdruckgabe aufgefordert zu werden, oder auch, im Falle der Autorin, trotz eines inneren, in jenem Moment keinesfalls einfach zu explizierenden, Unbehagens, Daten des Fingerabdrucks für ein bargeldloses Bezahlverfahren *frei-*

[45] Ergebnisse hierzu hat Jana Böger, die als studentische Hilfskraft im Projekt beschäftigt war, 2012 im Rahmen ihrer Masterarbeit vorgelegt, in der sie Darstellungsweisen der Fingerabdrucktechnologie anhand von Werbematerialien diverser Anbieter untersucht hat.

willig preiszugeben, um der Forderung nach Vertrautheit mit dem untersuchten Feld nachzukommen.

2.1.3 Qualitative Interviews mit Fingerabdruckgebern

Ergänzend zu den Beobachtungen wurden qualitative Interviews mit Nutzern durchgeführt. Die forschungsleitenden Fragen legten ein qualitatives Interviewverfahren nahe, das der Forderung nach Offenheit einer verstehenden Herangehensweise im Forschungsprojekt, aber auch, angesichts der theoretischen Vorannahmen, jener nach problembezogener Rahmung gerecht wird (vgl. Hopf 1991: 180f.). Zu solch „diskursiv-dialogischen" (Mey/Mruck 2007: 252) Interviewverfahren gehört das problemzentrierte Interview von Andreas Witzel (2000, 1985), an welches die Durchführung der Interviews angelehnt wurde. Die Geeignetheit des problemzentrierten Interviews, das unter anderem auf ethnomethodologischen Überlegungen und jenen Aaron Cicourels beruht und das Witzel (1985) in Abgrenzung zu narrativen Interviewverfahren entwickelt hat, begründet sich nicht nur durch die zugrunde gelegten Prinzipien von Offenheit, Kommunikation und Problemzentrierung – welche das theoretische Vorwissen des Forschers betonen –, sondern auch in der geteilten analytischen Zielrichtung, „Handlungsbegründungen und Situationsdeutungen, die Subjekte angesichts gesellschaftlicher Anforderungen formulieren" (ebd.: 228), zu ergründen. Explizit erwähnt Witzel (ebd.: 230), dass dazu auch „die objektiven Rahmenbedingungen zu untersuchen [sind], von denen die betroffenen Individuen abhängig sind, die sie in ihrem Handeln berücksichtigen und für ihre Absichten interpretieren müssen". Zentrales Element des problemzentrierten Interviews ist das entlang eines Leitfadens organisierte qualitative Interview selbst, das gleichwohl in der ursprünglichen Form des problemzentrierten Interviews (vgl. ebd.: 235ff.) nur ein Element unter vielen darstellt und von Witzel (ebd.) mit anderen Erhebungs- und Auswertungsmethoden, wie die Fallanalyse, die biographische Methode oder die Gruppendiskussion, kombiniert wird – Methoden, die im Projekt keine Anwendung gefunden haben.

Die Bedeutung eines offenen, entlang eines Leitfadens thematisch-strukturierten Interviewverfahrens für die Studie ist konkret darin zu sehen, dass es, auf der einen Seite, eine Orientierung an eben jenem theoretischen Vorwissen ermöglicht, weil mit ihm die als relevant erachteten Gesichtspunkte und Dimensionen erfasst und abgefragt sowie aus Beobachtungssituationen stammende Deutungen im Gespräch – im Sinne einer Erweiterung und Vervollständigung (vgl. Flick 1985: 251) – kommunikativ validiert werden können. Der Leitfaden ist somit das zentrale Instrument des Interviewverfahrens: Er „soll das Hintergrundwissen des

Forschers thematisch organisieren, um zu einer kontrollierten und vergleichbaren Herangehensweise an den Forschungsgegenstand zu kommen.“ (Witzel 1985: 236) Demgegenüber ermöglichen an Leitfragen orientierte Interviewformen aber immer auch einen „Kommunikationsprozess“ (Gläser/Laudel 2010: 111), in dem die Befragten in die Situation versetzt werden, selbst „aktiv Ereignisse, Erfahrungen, Handlungen und Wissen zu rekonstruieren“ (Honer 2003: 95) und so auch unerwartete, ihnen gleichsam wichtige Aspekte zur Sprache bringen können.

Da das Projekt an den „Sinndeutungen“ (Diekmann 2000: 444) der Befragten interessiert war, wurden die forschungsleitenden Annahmen für den Leitfaden in Interviewfragen übersetzt, die sowohl argumentationsanregende als auch erzählgenerierende Impulse für die Gespräche mit den in den unterschiedlichen Settings befragten Nutzern bereithielten (vgl. Anhang A). Die Leitfäden orientieren sich an drei großen Themenkomplexen: (1) der Situation der Registrierung der Fingerabdruckdaten, (2) den Bedeutungszuschreibungen zur Technologie im Allgemeinen, innerhalb der jeweiligen Sozio-Praktik und im Umgang mit der Technik sowie (3) Einschätzungen zur Anwendung der Fingerabdrucktechnologien in anderen Anwendungssettings. Die konkreten Fragen innerhalb der Themenkomplexe dienten dabei als Orientierung im Interview und wurden entsprechend des Postulats von Offenheit und dem Ziel, eine möglichst natürliche Gesprächssituation zu schaffen, ‚unbürokratisch‘ (in Anlehnung an Hopf 2005: 358 mit Bezug auf dies. 1978) entsprechend der jeweiligen Gesprächssituation gestellt. Trotz dieser Flexibilität sichert ein Leitfaden so eine „Vergleichbarkeit mit anderen Interviews, denen der gleiche Leitfaden zugrunde liegt“ (Marotzki 2003: 114). Gleichwohl eingesetzt wurden jeweils kontextspezifische Leitfäden, das heißt unter Beibehaltung der Hauptthemenkomplexe enthielten diese teilweise identische, teilweise unterschiedliche Fragen. Dass die Modifikation der Leitfäden primär entlang in der Beobachtungsphase gewonnener Informationen in den unterschiedlichen Settings erfolgte entspricht dem reflexiven Charakter des Instruments, theoretische Vorannahmen den Beobachtungen und ersten Befunden und letztlich der Wirklichkeit der Befragten anzupassen. Die Interviews wurden mit dem Einverständnis der Befragten digital aufgezeichnet und anschließend anonymisiert. Ihre Transkription erfolgte, in Anlehnung an die Regeln von Froschauer und Lueger (2003), analog zur literarischen Umschrift, das heißt entsprechend der Standardsprache bzw. des Dialektes wurden die Interviews, unter Verzicht von Prosodie und Überlappungen, wörtlich transkribiert.

2.2 Die Durchführung der Erhebungen

Die nachfolgende Beschreibung der etwa 14 Monate andauernden Erhebungen dient zugleich der Explikation der Auswahlkriterien des Samplings sowie einer ersten Beschreibung der ausgewählten Untersuchungssettings.

Arztpraxis

Den Beginn der Erhebungsphase markierten zwei Interviews, die im April und Oktober 2010 zum Pretest des Interviewleitfadens mit zwei Angestellten in einer privaten Zahnarztartpraxis mit 16 Mitarbeitern in einer norddeutschen Großstadt durchgeführt wurden. In diesem Setting wurde für wenige Monate ein Fingerabdruckverfahren zu Zeiterfassungszwecken eingesetzt. Die Entscheidung erstmals ein Zeiterfassungssystem zu installieren geht, einerseits, auf die Forderung eines Teils der Arbeitnehmer zurück, innerbetriebliche Gerechtigkeit bei der Einhaltung von Arbeitszeiten, mithin eine Kontrolle über Anwesenheit zu ermöglichen, die der leitende Arzt der Praxis aufgrund seiner Teilzeittätigkeit nicht gewährleisten kann. Die Installation des Fingerabdrucksystems für diese Zwecke basiert, andererseits, auf der Entscheidung des Arbeitgebers, der dies mit der Anschlussfähigkeit des Systems an die installierte Praxissoftware begründet. Dem leitenden Arzt obliegt die Durchführung der Erstregistrierungen – die Daten werden auf einem lokalen Server gespeichert – sowie die Verwaltung des Systems. Arbeitnehmer meldeten sich bei Arbeitsbeginn an dem System an und bei Dienstschluss von diesem ab. Zum Zeitpunkt der Befragungen war das System allerdings nicht länger in Betrieb, sodass Beobachtungen hier nicht stattfinden konnten.

24-Stunden- bzw. Automaten-Videothek

Die ersten Beobachtungen begannen im November 2010 in einer 24-Stunden-Videothek, in der das Fingerabdruckverfahren als Mittel der Zugangsbeschränkung, das heißt als obligatorisches Verfahren zur Authentifizierung der Kunden an den DVD-Verleihautomaten fungiert. Die Videothek befindet sich in einer weiteren norddeutschen Großstadt und dort in einem heterogenen Stadtteil, der von der Bausubstanz, den alteingesessenen Geschäften und Ladenlokalen in der fußläufigen Umgebung der Videothek sowie den im Straßenbild präsenten PKW an ein kleinbürgerliches Arbeiter- und Angestelltenquartier erinnert. Die seit sieben Jahren inhabergeführte Automatenvideothek ist zum Zeitpunkt der Beobachtungen in einem Umkreis von einem Kilometer nicht nur die einzige Videothek, sondern in diesem bzw. angren-

zenden Stadtteilen die einzige Automatenvideothek, die 24 Stunden am Tag und 365 Tage im Jahr geöffnet ist. Ansprechpartner für die Erstregistrierung ist der Inhaber selbst, der keine weiteren Mitarbeiter beschäftigt. Bei der Videothek handelt es sich um ein Ladenlokal, das aus einem einzigen Raum besteht, welcher sich in einen öffentlich zugänglichen, etwa 15qm großen, Bereich sowie ein nicht einsehbares Büro des Inhabers aufteilt. Die großen Schaufenster des kleinen Raums sind überwiegend durch Filmplakate bzw. Filmtafeln zugehängt, sodass der Einblick von außen resp. umgekehrt eingeschränkt ist. Zugang zum Ladenlokal erhalten die Nutzer mittels einer Magnetkarte, auf der Name und Guthaben der Kunden gespeichert sind. Diese Karte öffnet nicht nur die Eingangstür, sondern dient auch dazu, sich an den drei, tief in eine Wand eingelassenen, Ausleihautomaten anzumelden. In diese, höhlenartig anmutenden, Automaten müssen sich die Nutzer hineinlehnen um auf einem Monitor ihre Filmauswahl zu treffen und den Automaten und daran befindlichen Fingerabdruckscanner zu bedienen.[46] Nach erfolgreicher Authentifizierung erhalten die Kunden den gewählten Film über einen Ausgabeschacht am Automaten. Über einen weiteren Schacht erfolgt die Rückgabe der Filme. Registrierte Kunden können zudem auf der videothekeneigenen Homepage mit einem persönlichen Code Filme vorbestellen und ohne Verwendung des Fingerabdruckverfahrens in der Videothek abholen.

Zum Zeitpunkt der Beobachtungen sind etwa 2.600 Kunden in der Videothek registriert, von denen im Februar 2011 wiederum etwa 450 als aktive Nutzer gelten. Die heterogene, sich in den geführten Interviews widerspiegelnde, Altersstruktur der Nutzer liegt etwa zwischen 18 und 60 Jahren und in der Regel kommen die Nutzer aus der näheren Umgebung der Videothek. Die Beobachtungen wurden an jeweils zwei Wochentagen zwischen 15 und 20 Uhr durchgeführt, an denen auch der Inhaber regelmäßig und verlässlich vor Ort ist, um Registrierungen vorzunehmen oder um für Fragen oder bei Problemen zur Verfügung zu stehen. Während der sechstägigen Beobachtungen in der Videothek meldeten sich insgesamt acht Personen für das Verfahren an, von denen sich drei Personen für ein Interview zur Verfügung stellten. Weitere zehn Mal konnte der Ausleihvorgang per Fingerabdruck beobachtet und mit sechs dieser Bestandskunden ein Interview geführt werden. Eine sich in den Beobachtungen andeutende Tendenz, dass bei langjährig etablierten Anwendungen die Zahl neuer Nutzer stagniert und/oder diese deutlich weniger aktiv genutzt werden, als Personen registriert sind, zeigte sich ebenfalls im Anwendungssetting Supermarkt, das als ein Beispiel für ein Bezahlverfahren ausgewählt wurde.

[46] Diese baulich determinierte Diskretion, die etwa verhindert, dass andere Kunden die persönliche Filmauswahl einsehen können, steht im Gegensatz zu der Installation von zwei Videoüberwachungskameras, die große Teile des Raumes erfassen.

Supermarkt

In dem ausgewählten Verbrauchermarkt, der etwa zwei Kilometer vom Stadtkern entfernt an einer Hauptstraße eines Wohngebiets mit Einzel- und Mehrfamilienhäusern in einer süddeutschen Mittelstadt liegt, ist die Bezahlung mit dem Fingerabdruck eine bereits seit einigen Jahren etablierte Alternative zur Geldkarten- beziehungsweise Barzahlung. In diesem Stadtteil, der im Vergleich die höchste Bevölkerungsdichte im Stadtkreis aufweist, gibt es nur wenige Einrichtungen des öffentlichen Lebens. Im fußläufigen Umkreis des Supermarktes etwa befinden sich lediglich ein Eiscafé, eine Bäckerei sowie einige wenige Einzelhandelsgeschäfte und alternative Einkaufsmöglichkeiten liegen, mit einer Ausnahme, in mindestens sechs Kilometern Entfernung. Der privat geführte Verbrauchermarkt mit über 50-jähriger Geschichte im Ort, der bereits in der dritten Generation geführt wird, ist mit knapp 1.000qm Verkaufsfläche zwar überschaubarer als andere ansässige Hypermärkte mit einer Mindestgröße von mindestens 5.000qm, bietet allerdings als Markt im Bereich des Lebensmittelvollsortiments eine größere Angebotsvielfalt als Discounter-Märkte. Den Supermarkt kennzeichnet ein hohes Engagement für Kundenbindung: im Eingangsbereich des Markts liegen zahlreiche Rabattcoupons, Marktzeitungen und Hinweise auf Werbespiele aus. Er ist aufgrund einer hohen Barrierefreiheit zudem als „seniorenfreundlicher Markt“ ausgezeichnet. An allen vier Kassen besteht die Möglichkeit mit dem Fingerabdruckverfahren zu bezahlen. Die mobilen Fingerabdruckscanner befinden sich, ebenso wie das mobile EC-Karten-Lesegerät, unauffällig neben den Supermarktkassen und werden nach Bedarf von den Mitarbeitern zur Bezahlung gereicht. Die Registrierung für das Fingerabdruckverfahren selbst findet im Büro des Marktleiters an einem Computer mit angeschlossenem Fingerabdruckscanner statt. Gespeichert werden die Daten in einer zentralen Datenbank, um das Rücklastschriftverfahren zu gewährleisten. Die finanzielle Investition in das Fingerabdrucksystem ist für den Inhaber primär durch sein Interesse an der Verringerung von Transaktionskosten motiviert, die mit anderen Bezahlverfahren verbunden sind. Wuchs mit der offiziellen Einführung des Fingerabdruckverfahrens Mitte der 2000er Jahre in der Filiale die ursprünglich anvisierte Kundenzahl von 100 im selben Jahr auf 250, konnte die zum Zeitpunkt der Beobachtungen tatsächlich registrierte Anzahl von Kunden weder vom Inhaber, noch dem mit der Neuregistrierung beauftragten Marktleiter benannt werden. Zum Zeitpunkt der Beobachtungen ist nach Aussage des Inhabers die Zahl der Registrierungen für das Verfahren auf etwa zwei Kunden pro Monat stagniert und wird auf eine Ausschöpfung der am Verfahren interessierten Klientel vor Ort zurückgeführt. Wurden potentielle Nutzer bei der Einführung des Verfahrens vor allem durch den Inhaber persönlich oder das Kassenpersonal angesprochen, erfolgt eine solche Bewerbung des Verfahren oder durch

Flyer nur noch selten. Da man in diesem Setting vor allem auf Mundpropaganda: „von Kunde zu Kunde“ (Guido Boll, Sm) setze, zeigte sich in diesem Setting in besonderer Weise, dass die Frage danach, wie man Zugang zum Feld erhält, bereits seine Charakteristika selbst schließen lässt (Lüders 2005: 392): Angesichts der vom Inhaber als gering beschriebenen Registrierungsquote erfolgte die Einladung für die Beobachtungen im Rahmen einer, in einer Lokalzeitung angekündigten, zweitägigen Werbeaktion für das Verfahren, die an einen 5-Euro-Gutschein für den Einkauf im Supermarkt gekoppelt war und an einem Freitag und Sonnabend stattfand. An diesen Tagen betreute eine Werkstudentin einen Infotisch vor dem Supermarkt. Sie sollte nicht nur über das Verfahren informieren, sondern bat zudem Kunden um die Teilnahme an einer standardisierten Befragung im Rahmen ihrer Abschlussarbeit. Ihre Informationen zum Verfahren beschränkten sich in der Regel auf den Hinweis auf eine beschleunigte Zahlungsweise unabhängig von EC-Karte oder Bargeld. Konnten im Rahmen dieses Werbesettings insgesamt sieben Neuregistrierungen von Kunden, deren Alter zwischen 50 und Ende 70 lag, beobachtet werden, mit denen in sechs Fällen im Anschluss Interviews stattfanden, liegt vor diesem Hintergrund der Einwand potentieller Verzerrungen bei der Auswahl von Interviewten gleichwohl klar auf der Hand. Allerdings zeigen die Beobachtungen, dass die explizite Bewerbung des Bezahlverfahrens weniger Einfluss auf eine Registrierungsabsicht, als vielmehr auf den tatsächlichen Zeitpunkt der Registrierung hatte. So kamen fünf der bei der Registrierung beobachteten Kunden bereits mit einer klaren Registrierungsabsicht in den Supermarkt, das heißt ohne weitere Information von der Standbetreuerin einzuholen. Auch zeigten die Beobachtungen am Informationstisch, dass der für die Registrierung in Aussicht gestellte Gutschein viele von der Studentin angesprochene Kunden, die das Verfahren im Supermarkt bislang noch nicht kannten, nicht zu überzeugen vermochte, weil man „das wegen der fünf Euro jetzt nicht“ mache. Ist in dieser Hinsicht eine Abhängigkeit vom Ansprechverhalten der Studentin eher als gering zu bewerten, scheint sie sich gleichwohl im Interviewsample widerzuspiegeln, weil diese nicht nur etwa lediglich jeden zehnten Kunden, sondern vor allem ältere Menschen ansprach. Allerdings ließ sich vor allem tagsüber eine generelle Überalterung der Kundschaft in diesem Supermarkt feststellen, sodass auch hier Verzerrungseffekte eventuell als gering einzustufen sind.

Überraschend vor dem Hintergrund der im Vergleich zur durchschnittlichen Registrierungszahl eher hohen Neuanmeldungen und bereits registrierter Kunden war, dass das Bezahlen mit dem Fingerabdruck während der zwei Beobachtungstage insgesamt nur viermal beobachtet werden konnte.

Schulen

Ein vergleichbares ‚Missverhältnis' zwischen erfolgter Registrierung und tatsächlicher Benutzung zeigte sich auch während der Beobachtungen in zwei Schulen in einer weiteren süddeutschen mittelgroßen Stadt, in der vor wenigen Jahren mit der Einführung von Schulverpflegung auch ein Fingerabdruckverfahren als bargeldloses Bezahlverfahren in nahezu allen Schulkantinen implementiert worden ist. Es wurden für die Untersuchung ein Gymnasium im Stadtzentrum sowie eine Grund-, Haupt- und Realschule am Rande der Stadt ausgewählt. Das Gymnasium ist mit über 1.000 Schülern das größte der Stadt und verfügt über eine über 100-jährige Geschichte in diesem Standort. Es liegt nahe des Zentrums in einem Stadtteil, der sich sowohl durch seine Gründerzeitarchitektur und entsprechend sanierte Wohngebäude in der Nachbarschaft auszeichnet, als auch dadurch, dass Kioske, Cafés und Imbisse sowie Restaurants fußläufig zu erreichen sind. Die Grund-, Haupt- und Realschule mit insgesamt 600 Schülern entstand demgegenüber erst in den 1950er Jahren und liegt inmitten eines Wohngebietes mit einer hohen Bevölkerungsdichte und einer, im Vergleich zur innerstädtischen Lage des Gymnasiums, überschaubaren infrastrukturellen Ausstattung. In unmittelbarer Umgebung der Schule gibt es lediglich einen Kiosk mit angeschlossenem Café.

Die Nutzung des ursprünglich für alle Schüler verpflichtend geplanten bargeldlosen Bezahlverfahren ist, aufgrund politischer Widerstände, zum Zeitpunkt der Beobachtungen ausschließlich für Bezieher von Arbeitslosengeld II beziehungsweise Berechtigte für dort übliche Familienpässe, alternativ zu einem aufladbaren RFID-Chip, der gegen eine Schutzgebühr von 5€ ausgegeben wird, verpflichtend, um von Essenssubventionen profitieren zu können. Sowohl das biometrische als auch das nicht biometrische bargeldlose Bezahlsystem sind über ein Treuhandkonto organisiert, für das im Vorhinein eine Onlineanmeldung erforderlich ist. Unabhängig vom Status eventueller Vergünstigungen müssen die Eltern der Schulkinder nicht festgelegte Beträge auf das Konto überweisen, von dem aus dann direkt das Geld für die jeweiligen Essenskäufe abgebucht wird. Kontostände und entsprechende Abrechnungen sind für die Nutzer online einsehbar bzw. werden per E-Mail-Benachrichtigungen kommuniziert. Eltern haben mit der Nutzung des Systems außerdem die Möglichkeit eine Kontingentierung der täglichen Ausgaben ihrer Kinder zu verfügen. Eine solche Festsetzung der Ausgabenlimits kann sich sowohl auf die Art der Mahlzeit – Zwischenmahlzeiten und/oder Mittagessen – als auch auf die tägliche Höhe der Ausgaben in der Schulkantine beziehen.

Das Einlesen der Daten für das Fingerabdruckverfahren erfolgt zum Zeitpunkt der Beobachtungen in den jeweiligen Schulmensen und wird durch das dortige Personal der Catering-

Firma, welche das Verfahren auch verwaltet, durchgeführt. In beiden Schulen, und damit vergleichbar der Platzierung im Supermarkt, befinden sich die Fingerabdruckscanner direkt neben den Kassen in der Mensa. Laut eines Artikels einer lokalen Tageszeitung aus dem Jahr 2009 sind von den zu diesem Zeitpunkt 4.500 Schülern an allen Schulen der Stadt in knapp 3.000 Fällen Fingerabdruckdaten gespeichert worden. Davon hätten schließlich auch 1.529 Eltern ein Treuhandkonto eröffnet. Würden dem Artikel zufolge 75 Prozent der ausgegebenen Essen mit dem Fingerabdruck bezahlt, zeigen die Beobachtungsdaten ein anderes Bild: Auch wenn die genaue Anzahl registrierter Schüler in den jeweiligen Schulen zum Zeitpunkt der Beobachtungen nicht zu ermitteln war – der Schulleiter des Gymnasiums schätzt, dass etwa ein Drittel der Schüler das Fingerabdrucksystem nutzen würden –, scheinen gleichwohl die Relationen umgekehrt zu sein. In beiden Schulen benutzen den Beobachtungen zufolge lediglich jeweils 20 bis 30 Schüler täglich das Verfahren. An vier Tagen protokollierten wir in beiden Schulmensen so insgesamt 108 Mal das Bezahlen mit dem Fingerabdruck.

Diese Beobachtungen wurden, ebenso wie die Möglichkeiten zur Teilnahme an Interviews, in Absprache mit den jeweiligen Schulleitungen Schülern und Eltern im Vorfeld schriftlich angekündigt. Eine direkte Ansprache der Schüler in Pausen erfolgte nur selten. Während in der Grund-, Haupt- und Realschule die Lehrerschaft die Organisation der Interviewtermine anhand eines Informations- und Einwilligungsformular für Interviewtermine übernahm, sodass auf diese Weise sieben Interviews mit Kindern zwischen 7 und 12 Jahren sowie mit zwei Eltern vermittelt wurden, bot sich im Gymnasium im Anschluss an eine Einführungsveranstaltung, in der die Projektarbeiter ihr Vorhaben vorstellten, die Möglichkeit, acht Interviews mit Schülern zwischen 12 und 18 Jahren und vier Interviews mit Eltern durchzuführen, unabhängig davon, ob das Verfahren bereits genutzt oder eine Anmeldung erst noch erwogen wurde.

Einwohnermeldeamt

Ein weiteres für das Projekt zentrales Untersuchungssetting bildete die Aufnahme und Speicherung des Fingerabdrucks in Ausweispapieren, konkret im ePass und dem neuen Personalausweis. Die Untersuchung fand in einer Referenzbehörde einer norddeutschen Großstadt statt. Das offiziell als Kundenzentrum bezeichnete Amt liegt im Stadtkern in unmittelbarer Nähe zu zahlreichen Einzelhandelsgeschäften und Restaurants sowie zahlreichen Anbindungen an den öffentlichen Nahverkehr und ist, außer für Ausweisdokumente, auch für alle anderen behördlichen Leistungen, etwas Ummeldungen oder Beglaubigungen, zuständig. Das Einwohnermeldeamt ist – wie viele öffentliche Ämter in deutschen Städten – vor einigen Jah-

ren zum Großraumbüro umgebaut worden. Es verfügt über sieben Arbeitsplätze, mit jeweils zwei Stühlen für die Antragsteller, die flexibel von den Sachbearbeitern genutzt werden können. Auf den, weitestgehend leeren, Schreibtischen – die Angestellten haben jeweils abschließbare, individuelle Wägelchen, mit denen sie zwischen den Arbeitsplätzen wechseln – steht neben dem PC-Bildschirm deutlich sichtbar der Fingerabdruckscanner. Dem Hinweis des Kundenzentrumsleiters folgend, dass Montag und Donnerstag zum Zeitpunkt der Beobachtungen die am häufigsten von Kunden frequentierten Tage sind – täglich kämen etwa 500 Kunden, von denen 25 bis 30 Prozent Dokumentenantragsteller seien –, fanden nur an diesen Wochentagen Beobachtungen statt. An insgesamt drei Tagen konnten so bei verschiedenen Bezirksamtsmitarbeitern Beobachtungen von insgesamt 46 Antragstellungen von Identitätsdokumenten in der Meldebehörde (18 Beantragungen eines Reisepasses, 28 Beantragungen eines Personalausweises)[47] protokolliert werden. Im Anschluss an die Beobachtungen, die direkt am Schreibtisch der Mitarbeiter erfolgten, wurden mit insgesamt 23 Personen zwischen 21 und 77 Jahren, darunter vier Ehepaare, insgesamt 19 Interviews durchgeführt. Von diesen Befragten beantragten zehn einen Reisepass und zwei von ihnen zugleich auch einen neuen Personalausweis. Für eine Aufnahme der Fingerabdrücke in den neuen Personalausweis entschieden sich insgesamt zehn der Befragten, fünf Personen lehnten dies ab. Trotz einer eher geringen Nutzung des Verfahrens in den einzelnen Settings konnten insgesamt 185 Vorgänge (vgl. Tab. 4) beobachtet und 57 Interviews durchgeführt werden (vgl. Tabelle 5 bis 10, Tabelle 11 stellt eine Übersicht über die Interviews mit Fingerabdrucknehmern dar).

[47] In 33 Fällen wurden die Fingerabdruckdaten in die Dokumente aufgenommen, davon 15-mal im Rahmen der Beantragung eines Personalausweises.

Tabelle 4: Umfang der Erhebungen

	Arzt-praxis	**Videothek [Vid]**	**Supermarkt [Sm]**	**Gymnasium [Schul1]**	**Grund-, Haupt-, Realschule [Schul2]**	**Einwohner-meldeamt [Einwo]**
Erhebungs-zeitraum	08-10/2010	11/2010-01/2011	05/2011	09/2011	10/2011	11/2011-01/2012
Beobachtungs-tage	-	6	2	2	2	3
Beobachtete Vorgänge	-	18 davon 8 Neu-registrierun-gen	12 davon 7 Neu-registrierun-gen	67 davon 0 Neuregistrie-rungen	42 davon 0 Neuregistrierungen	46 Antragstel-lungen, davon 31 Re-gistrierungen
Interviews mit Fingerab-drucknehmern	2 Inter-views	9 Interviews	6 Interviews	4 Interviews mit Eltern 8 Interviews mit Kin-dern/Jugendlic hen	2 Interviews mit Eltern 7 Interviews mit Kin-dern/Jugendlichen	19 Interviews

Tabelle 5: Interviews im Setting Arztpraxis (Arzt)

Befragte	**Alter**	**Nutzung**
Nicole Kunze	32 Jahre	Nutzt das Verfahren nicht mehr
Kathleen Häuser	35 Jahre	Nutzt das Verfahren nicht mehr

Tabelle 6: Interviews im Setting Videothek (Vid)

Befragte	**Alter**	**Nutzung**
Anton Borowski	60 Jahre	Nutzt das Verfahren
Corinna Meier	28 Jahre	Nutzt das Verfahren
Florian Grippe	28 Jahre	Nutzt das Verfahren
Karsten Gald	38 Jahre	Nutzt das Verfahren
Julia Franke	20 Jahre	Nutzt das Verfahren
Max Schaf	23 Jahre	Nutzt das Verfahren
Katrin Milcher	33 Jahre	Nutzt das Verfahren
Aznar de Silva	33 Jahre	Nutzt das Verfahren
Rainer Tapfer	44 Jahre	Nutzt das Verfahren

Tabelle 7: Interviews im Setting Supermarkt (Sm)

Befragte	**Alter**	**Nutzung**
Karl Baumann	70 Jahre	Nutzt das Verfahren
Rolf Burger	50 Jahre	Nutzt das Verfahren
Erika Hundt	63 Jahre	Nutzt das Verfahren
Burghard Eisen	77 Jahre	Nutzt das Verfahren
Petra Müller	56 Jahre	Nutzt das Verfahren
Peter Wagner	65 Jahre	Nutzt das Verfahren

Tabelle 8: Interviews im Setting Schule - Gymnasium (Schul1)

Befragte	**Alter**	**Nutzung**
Schüler		
Felix Stäubner	16 Jahre	Nutzt das Verfahren
Malte Günthner	17 Jahre	Nutzt das Verfahren
Maria Reckling	12 Jahre	Nutzt das Verfahren
Steffi Drobnic	12 Jahre	Erwägt eine Nutzung
Merle Jürgens	13 Jahre	Plant eine Nutzung
Jessica Schütt	13 Jahre	Nutzt das Verfahren
Mira Soeffner	18 Jahre	Nutzt das Verfahren nicht mehr
Simone Kutzer	17 Jahre	Nutzt das Verfahren
Sören Berger	16 Jahre	Nutzt das Verfahren
Theresa Valentin Lena Brink *(Freundinnen, gemeinsam befragt)*	14 Jahre 14 Jahre	Nutzt das Verfahren Nutzt das Verfahren nicht
Eltern		
Wolfgang Flieger	50 Jahre	Sohn nutzt das Verfahren
Christa Jürgens	45 Jahre	Tochter erwägt Nutzung
Monika Reckling	40 Jahre	Sohn und Tochter nutzen das Verfahren
Hartmut Weber Klaudia Michaelis Jens Thiele *(gemeinsam befragt)*	45 Jahre 45 Jahre 45 Jahre	Erwägen Nutzung für ihre Kinder

Tabelle 9: Interviews im Setting Schule - Grund-, Haupt-, Realschule (Schul2)

Befragte	**Alter**	**Nutzung**
Schüler		
Amelie Cerni Frederike Cerni *(Schwestern, gemeinsam befragt)*	8 Jahre 8 Jahre	Nutzt das Verfahren Nutzt das Verfahren
Giovanni Pirlo	12 Jahre	Nutzt das Verfahren nicht mehr
Luca Michaelis	9 Jahre	Nutzt das Verfahren
Magdalena Kirchner	7 Jahre	Nutzt das Verfahren
Pascal Pradhan	9 Jahre	Nutzt das Verfahren
Pinar Erding	10 Jahre	Nutzt das Verfahren
Vanessa Klein	12 Jahre	Nutzt das Verfahren
Eltern		
Thea Pirlo	45 Jahre	Sohn nutzt das Verfahren nicht mehr
Sabine Walter	35 Jahre	Sohn nutzt das Verfahren

Tabelle 10: Interviews im Setting Einwohnermeldeamt (Einwo)

Befragte	**Alter**	**Nutzung**
Veronika Amarell	45 Jahre	Personalausweis mit Fingerabdrücken
Greta Böttcher	75 Jahre	Personalausweis mit Fingerabdrücken
Sybille Brandt	45 Jahre	ePass
Niko Heidrich	30 Jahre	ePass
Thorsten Hildesheimer	50 Jahre	ePass
Hans-Peter Janßen Gudrun Janßen *(Ehepaar, gemeinsam befragt)*	73 Jahre 70 Jahre	Personalausweis mit Fingerabdrücken Personalausweis mit Fingerabdrücken
Susanne Jeske	21 Jahre	Personalausweis mit Fingerabdrücken
Anita Kohlberg	55 Jahre	ePass
Günther Konrad	65 Jahre	Personalausweis mit Fingerabdrücken
Thomas Lambrecht	28 Jahre	Personalausweis ohne Fingerabdrücke
Dietmar Lemke	45 Jahre	ePass
Stephan Löw	28 Jahre	Personalausweis ohne Fingerabdrücke
Veronika Oppermann Rüdiger Oppermann *(Ehepaar, gemeinsam befragt)*	65 Jahre 68 Jahre	ePass Personalausweis mit Fingerabdrücken ePass
Eberhard Pelzig Ilona Pelzig *(Ehepaar, gemeinsam befragt)*	75 Jahre 75 Jahre	Personalausweis mit Fingerabdrücken Personalausweis ohne Fingerabdrücke
Alfons Petersen Louise Petersen *(Ehepaar, gemeinsam befragt)*	77 Jahre 77 Jahre	ePass ePass Personalausweis ohne Fingerabdrücke
Doris Ulmer	40 Jahre	Personalausweis mit Fingerabdrücken
Carsten Welzer	25 Jahre	ePass
Angelika Wilde	45 Jahre	Personalausweis ohne Fingerabdrücke
Christian Zander	48 Jahre	Personalausweis mit Fingerabdrücken

Tabelle 11: Interviews mit „Fingerabdrucknehmern“[48]

Befragte	**Alter**	**Funktion**
Michael Clausthal	45 Jahre	Inhaber der Arztpraxis
Andre Behringer	42 Jahre	Inhaber der Automatenvideothek
Guido Boll	56 Jahre	Inhaber des Supermarktes
Tobias Möhring	51 Jahre	Schulleiter des Gymnasiums (Schul1)
Katja Werner	30 Jahre	Mensaleiterin und Kassiererin im Gymnasium (Schul1)
Detlef Moltenkamp	45 Jahre	Schulleiter der Grund-, Haupt- und Realschule (Schul2)
Dagmar Stoltenberg	33 Jahre	Kassiererin in der der Grund-, Haupt- und Realschule (Schul2)
Rüdiger Heinz	40 Jahre	Fachbereichsleiter des Kundenzentrums im Einwohnermeldeamt

[48] Die Bezeichnung Fingerabdrucknehmer bezieht sich, wie in Kapitel 2.1.2 dargestellt, sowohl auf Personen, die Registrierungsprozesse vornehmen oder Nutzungsprozesse begleiten, als auch auf Betreiber der jeweiligen Einrichtungen.

2.3 Die Analyse des Materials

Die Entscheidung für ein Analyseverfahren in der qualitativen Forschung wird je nach dem zu untersuchenden Gegenstand, aber auch in Abhängigkeit von den gewählten Erhebungsmethoden gewählt. Im Zentrum dieser Untersuchung steht die Rekonstruktion subjektiver Sinnzusammenhänge im Hinblick auf ein zu beobachtendes Handeln innerhalb eines spezifischen Anwendungssettings, in welchem, so die Ausgangsannahme des Projektes, interaktive Aushandlungsprozesse über die (zu akzeptierende) Technologie stattfinden. Statt also vorauszusetzen, dass die Bedeutung des Fingerabdruckverfahrens bereits feststünde, zielten sowohl die Beobachtungen der Registrierungs- und Nutzungsprozesse, als auch die anschließenden Befragungen der Nutzer zunächst darauf ab, zu ergründen, wie diese in der Interaktion mit dem Fingerabdrucknehmer hergestellt wird. Die Auswertung der Protokolle und Interviews, das heißt der analytische Umgang mit den Daten war angelehnt an die Analysepraxis der Grounded Theory (Glaser/Strauss 1998), welche zwar selbst „keine spezifische Methode oder Technik“ zur Verfügung stellt, dafür aber einen Forschungsstil kennzeichnet, „nach dem man Daten qualitativ analysiert und der auf eine Reihe von charakteristischen Merkmalen hinweist“ (Strauss 2004: 434), und in deren Mittelpunkt das Aufbrechen, Systematisieren und Konzeptualisieren der gewonnenen Daten steht. Der Beginn dieser Kodierarbeit war im Projekt zunächst gleichwohl weniger theoretisch (vgl. Flick 2007: 258ff.), als vielmehr thematisch angeleitet. Dieses Vorgehen folgte damit den methodischen Vorschlägen Uwe Flicks (2007, 1996), auf der Basis fallbezogener Analysen thematische Dimensionen, das heißt unter Einbezug theoretischer Vorüberlegungen, wie sie sich in der Sampling-Strategie widerspiegeln und den Befragten mit dem Leitfaden auferlegt waren, aufzuschlüsseln, um so zu fallübergreifenden Vergleichen zu gelangen (ebd. 2007: 271, 1996: 160f.). Dem thematischen Kodieren liegt dabei ein mehrstufiges, zirkulierend-lineares Vorgehen zugrunde. Es zielt auf eine gleichermaßen deduktive wie auch induktive Aufschlüsselung des Materials (ebd. 1996: 163), um den umfangreichen Datenkorpus interpretativ zu detaillieren und ihm zugleich eine deutliche Strukturierung zu verleihen. Zudem dienten erste Kurzbeschreibungen der Befragten (vgl. ebd. 2007: 272f., 1996: 161f.), die im Anschluss an die Interviews erstellt wurden – analog zu den Beobachtungsprotokollen –, einem ersten Aufschlüsseln der Daten. Auf diese Weise fanden so bereits als relevant erachtete Textstellen Eingang in die Beschreibungen und sensibilisierten für erste Gemeinsamkeiten und Unterschiede, aber auch Irritationen im Hinblick auf die Bedingungen, die die Bedeutung der Technologie begründen. Im Prozess der detaillierten Auseinandersetzung mit den Daten „eröffnete“ (Kuckartz 2010: 79) dann das offene Kodieren

der Protokolle und Interviews die Forschungsarbeit, indem den Daten Kodes zugewiesen wurden, die sowohl auf theoretischen Konzepten bzw. konzeptuellen Kategorien beruhten oder auch auf der Basis der eigensprachlich von den Befragten benutzten, so genannten In-Vivo-Codes, gebildet wurden und in eben solchen Kategorien resp. thematischen Bereichen mündeten. Umgesetzt wurden die Auswertungen mittels der Analysesoftware für qualitative Daten MaxQDA, die sich als Instrument für analytische Verfahren anbietet, in denen das Kodieren und die Kategorienbildung eine grundlegende Rolle spielen (ebd.: 13). Als heuristische Folie der Kodierung, sowohl der Interviews als auch der Beobachtungsprotokolle, dienten zunächst die als akzeptanzrelevant vermuteten „thematischen Felder" (Schütz/Luckmann 2003: 267). Das Ziel des thematischen Kodierens liegt nun darin, die konzeptionellen Zuordnungen am Einzelfall in einem vorläufigen Kategorienschema zusammenzuführen. Während der Bearbeitung weiterer Fälle – hier: zunächst innerhalb eines Settings und in einem weiteren Schritt, über das Setting hinaus – wird es sukzessive weiterentwickelt, das heißt immer wieder überprüft und modifiziert, bis es als theoretisch gesättigt gelten darf.

Für die vorliegende Arbeit ging mit dem Prozess des Aufgliederns und konzeptuellen Zusammenfügens gleichwohl statt einer theoretischen Sättigung ein Wandel des Forschungsinteresses und mit ihm eine Änderung des methodischen Vorgehens einher. Dieser gründete sich zunächst darin, dass sich die These des Forschungsprojektes entlang der erhobenen Daten nicht weiterverfolgen ließ. Wurde ursprünglich erwartet, dass Antragsteller bzw. potentielle Nutzer die Akzeptabilität des Fingerabdruckverfahrens in den jeweiligen Registrierungssituationen aushandeln, zeigten die Beobachtungen, erstens, dass eine solche Explizierungsarbeit („Articulation Work", Hornecker 2004: 17) sowohl von Seiten der Fingerabdrucknehmer, beispielsweise in Form längerer Ausführungen zu Sinn und Zweck, als auch der Fingerabdruckgeber, etwa durch konkrete Nachfragen, nur selten und wenn, dann auch nur punktuell stattfand. Dabei erfolgte die Organisation der Interaktionen in den einzelnen Settings, soweit sie zu beobachten war[49], durchaus regelhaft. In der Videothek wurden Informationen zur Funktionsweise des Automaten und der notwendigen Registrierungsmodalitäten innerhalb weniger Minuten und, im Regelbetrieb des DVD-Ausleihens, mitunter nebenbei erteilt. Im Rahmen eines Vertragsverschlusses erfolgten zunächst die Erfassung persönlicher Daten wie Name, Geburtsdatum und Personalausweisnummer der Kunden und die Ausstellung der Kundenkarte – für die ein Pfand von 10 Euro zu einrichten ist. Abschließend wurden am Ausleihautomaten die Daten eines Fingerabdrucks eingelesen. Im Supermarkt wurden die potentiellen Nutzer wortlos durch den Marktleiter in dessen Büro begleitet und hier erfolgte die Abfrage

[49] In den Settings Schule konnte keine Registrierung beobachtet werden.

persönlicher Daten wie Name, Geburtsdatum und Personalausweisnummer und Kontodaten sowie optional die Erfassung von Telefonnummer und Mailadresse. Die anschließende Speicherung der Fingerabdruckdaten verlief ohne weitere Erläuterungen, lediglich Hinweise zur Positionierung des Fingers auf dem Scanner wurden gegeben. Vergleichbar verlief die Registrierung der Fingerabdrücke in der Einwohnermeldebehörde: Einer Aktualisierung bzw. Aufnahme der für die Ausweispapiere erforderlichen Daten folgte in einem zweiten Schritt die Erfassung der Fingerabdrücke. Wurden diese für den ePass analog zu der vorherigen Datenaufnahme schlicht angekündigt, wurden Antragsteller für den Personalausweis um eine Einwilligung gebeten, die auf Nachfrage regelmäßig damit begründet wurde, dass es zur „Sicherheit sei“, aber „weder Vor- noch Nachteil“.

Obwohl die Situationen im Hinblick auf erwartete Aushandlungsprozesse ‚still‘ blieben, entfalteten die Befragten gleichwohl eine mitunter hochgradig ambivalente Haltung zur Technologie, wenn sie in den Interviews etwa (Un-)Sicherheit, Überwachung und Privatheit als ‚individuelle‘ Spannungsfelder verhandelten, deren Relevanz wiederum im Hinblick auf die jeweilige Einbettung der Technologie in ein bestimmtes Anwendungssetting variierte, da die Befragten auch zu Stellungnahmen bezüglich der Nutzung der Technologie in anderen Bereichen aufgefordert wurden. Gerade diese sich im Datenmaterial abzeichnende Perspektivität entzog sich einer eindeutigen thematischen Einordnung und schlug sich in der Fortentwicklung des Kategoriensystems (vgl. Abbildung 1) darin nieder, dass es nicht nur zu klären galt, *was* die Interviewten ansprachen. „Implizites Motiv“ (Berg/Milmeister 2008: 14) der Kategorisierung, auf einer eher formalen Ebene, wurde zudem die Differenzierung und Sortierung der Bezugspunkte dieser Thematisierungen, in anderen Worten, eine Analyse dessen, *worüber* etwa ausgesagt wurde, welche dann zu relevanten Konzepten der Untersuchung gerieten.

Folgen der Nutzung
Ambivalenz
- Positive Folgen
  - Sicherheit
  - Identität
  - Notfall
  - Dokumente
  - (…)
- Bequemlichkeit
- Kontrolle
- (…)
- Negative Folgen
- Missbrauch
- Verdacht
- Kontrollverluste
  - (…)

Neutrale Folgen
- Heterogene Nutzungszwecke
- Anonymität
- Missbrauch
- (…)

Bedeutung Fingerabdrucktechnologie
Fingerabdruck
- Beschaffenheit
  - Eindeutigkeit/Einmaligkeit
  - Unsichtbarkeit
  - (…)
- Risiko
- (…)

Technik

Interaktion
Situation
- Belastung
- Überraschung
- Normalität
- Zwang

Atmosphäre
Sicherheitsargumentationen
Informationsbedürfnisse
(…)

Setting
Routine
Lokalität
Vertrauen
Grenzen der Nutzung
Freiwilligkeit/Zwang
(…)

Interaktivität
Assoziationen
Routine
Funktionieren
Nicht-Funktionieren der Technik
- Praktische Konsequenzen
- Umgang
- Bewertung
- Handlungsstrategien
- Ursachenzuschreibung
- (…)

Abbildung 1: Ausschnitt aus der Struktur der Interviews (Kategoriensystem)

Mit einer, in Anlehnung an textlinguistische Verfahren, vorgenommenen Differenzierung (vgl. zur Thema-Rhema-Teilung Berg/Milmeister 2008) und der Suche nach solcherart sprachlichen „Indizien“ (ebd.: 11) erwies sich auf der inhaltlichen Ebene bereits allein das Thema Sicherheit als heterogenes und in Bezug auf seine prädikativen Bezüge vielfältiges. Eine weitere analytische Dimension erbrachte die Unterscheidung der in den Interviews vorliegenden Textsorten: so lagen sowohl Erzählungen über Erfahrungen und Erlebnisse als auch Argumentationen vor, das heißt Texte mit sowohl narrativ-episodischem und begrifflich-semantischem Wissen. Während sich ersteres eher auf Situationen, ihren Kontext und den entsprechenden Ablauf des Berichteten beziehen, abstrahiert die zweite Form davon und orientiert sich eher an Begriffen, Definitionen und Relationen. Für die Analyse der Bedeutungszuschreibungen zur und des Sinns der Technologie sensibilisierte diese Unterscheidung für die Relevanz der Technologie-Be-Deutung. So können Erzählungen für den Entstehungshin-

tergrund von Erfahrungen aufmerksam machen, während demgegenüber semantische Modelle des Wissens – etwa in Form von Schlüsselwörtern – auf eher abstrakteres Begriffs-und Regelwissen, also Verallgemeinerungen im Sinne von Normalitätserwartungen und Routinen rekurrieren. Der Vergleich dieser Textsorten ermöglichte insofern Fragen danach, inwiefern das ‚Normale', der „Hintergrund von Situationsannahmen" (Deppermann/Spranz-Fogasy 2001: 1157) seine Konkretisierung im Erlebten erfährt (Flick 2011: 28).

Insofern leitete den analytischen Umgang mit den im Datenmaterial aufscheinenden Ambivalenzen und Uneindeutigkeiten zunehmend ein hermeneutisch inspiriertes Vorgehen, mithin theoretisches Kodieren (vgl. Flick 2007: 258ff.), an, da sich die Frage nach der Erzeugung des verzweigten Reservoirs der Technologiebedeutung und den Bedingungen der impliziten Sinnsetzungen in den jeweiligen Settings neu stellte. Als hilfreich bei der Materialanalyse erwiesen sich in diesem Zusammenhang die im weitesten Sinne techniksoziologischen Ansätze, ebenso wie, teilweise mit ihnen verknüpft, praxistheoretische Einsichten (vgl. Kapitel 1.3.2). Es ging, erstens, darum zu ergründen, welche Bedeutung der Technologie zugeschrieben wird und dieses Wissen im Hinblick auf seine Erscheinungsformen und Erzeugungsprozesse sowie auf seine Phänomenstruktur (z.B. Thema, Merkmale, Ursache-Wirkungszusammenhänge) zu analysieren. Zweitens stellte sich die Frage, welche Rolle die in den Interviews zu Tage tretenden Ambivalenzen für eine Bestimmung der Akzeptanz spielen und entlang welcher Bedingungen sich diese für die Nutzer etwa tilgen lassen oder nicht. In diesem Zusammenhang galt es dann auch die Beobachtungsprotokolle erneut auf die sich in ihnen abbildenden Interaktions- und Handlungsstrukturen zu untersuchen. Die Suchbewegungen der Datenanalyse, die das weitere Kodieren anleiteten, waren in Anlehnung an gesprächsanalytische Einsichten (vgl. Deppermann 2008) unter anderem davon gelenkt, was darüber hinaus während der Registrierungs- und Nutzungsprozesse sowohl im Gespräch als auch im Umgang mit der Technik (nicht) *passierte*, in anderen Worten „wie [die] Gesprächsteilnehmer interaktiv relevante Realität konstituieren" (ebd.: 79, Herv. i.O.), denn

> „bestimmt ein Anwesender ohne Rücksicht auf die Aktivitäten anderer die maßgebliche Interpretation oder Gültigkeit von Äußerungen oder enthalten sich Gesprächsteilnehmer des Aushandelns von Bedeutungen, dann verweist dies zumeist auf ein sehr wichtiges Charakteristikum der Interaktion. Es kann sich dann um eine extrem asymmetrische, machtregulierte Interaktion handeln oder um einen ritualisierten Austausch, der für die Teilnehmer hochgradig voraussehbar ist." (ebd.: 71)

Die im Verlauf der Analyse des Datenmaterials hervortretenden Irritationen wurden aber nicht nur auf die bislang im Material identifizierten Aspekte und potentiellen Zusammenhänge, sondern auch auf das eigene Vorverständnis, welches seinen Ausdruck ja in den verwendeten

Erhebungsmethoden und vor allem den Leitfragen fand, angewendet. Es veranlasste eine kritische Auseinandersetzung mit den Vorannahmen des Projektes und insofern eine Situationsanalyse der eigenen Forschungstätigkeit selbst. Daraus resultierte, dass, statt die Akzeptanz also in der Verhandlung diskursimmanenter Akzeptabilitätskriterien zu verorten, sich mit der kritischen Reflexion jener diskursiven Verweisungen und mitunter normativen Bestimmungen der Technologie die Forschungsfrage stellte, wie Akzeptanz, mithin die Materialität des Objektes Fingerabdrucktechnologie auch fernab dieser Prämissen zu bestimmen sei. Mit dem Wissen um jene „Referenzdiversität“ (Berg/Milmeister 2008: 20) und im Anschluss an die Detailanalysen der sich im Kategoriensystem abbildenden Kode-Rubriken bzw. Konzepte richtete sich der Blick auf die sich zwischen ihnen abbildenden Verweisungszusammenhänge, die im empirischen Teil dieser Arbeit, analog zum axialen Kodieren bzw. der Logik des Kodierparadigmas der Grounded Theory (vgl. Strauss/Corbin 1996: 75ff.), für ein Verständnis der Akzeptanz zusammengefügt werden.

3 Zu den Bedingungen der Akzeptanz

Im Mittelpunkt dieses Kapitels stehen die empirischen Ergebnisse der Untersuchung, die sich, ausgehend von der Frage nach der Bedeutung der Technologie sukzessive den Nutzungsmotiven und den kontextuellen Bedingungen der Akzeptanz bzw. unterschiedlichen Ausprägungen dieser nähern.

3.1 Vom Objekt her besehen: Eine interpretativ flexible Technologie

„When faced with an object, attend first to the associations out of which it's made and only later look at how it has renewed the repertoire of social ties." (Latour 2005: 223)

Das Objekt der Akzeptanz in den Mittelpunkt der Betrachtung zu rücken bedeutet in diesem Kapitel seinem Eigensinn selbst nachzuspüren – ohne dabei jedoch, etwa im Sinne der Akteur-Netzwerk-Theorie, sein Handeln bzw. die der gegenständlichen Technik inhärenten Handlungsprogramme selbst zum Ausgangspunkt zu machen, würden so doch objektivierbare Handlungsbedingungen – als eines Umgangs mit ‚dem' Objekt – entworfen und die Frage der Akzeptanz geriete zu einer nach konkret identifizierbaren Faktoren einer beobachtbaren Nutzung der Technologie. Demgegenüber gilt es die Idee eines in gewisser Weise immer schon fertigen Objektes selbst zu befragen und damit Latours Aufruf im folgenden Kapitel vielmehr wortwörtlich zu nehmen: den Assoziationen nachzuspüren und die Realitäten des Objektes ‚Fingerabdrucktechnologie' aus der Perspektive ihrer Nutzer herauszuarbeiten.

Auf der Ebene der sich mit ihr verbindenden Zwecke bedeutet dies zunächst den Bedeutungszuschreibungen von „Bequemlichkeit" und „Sicherheit" zu folgen – Konnotationen, die nicht nur die Kernthemen des affirmativen als auch kritischen Biometrie-Diskurses bilden, sondern sich auf der Ebene der Interviews ebenfalls als die zentralen, gleichwohl inhaltlich differierenden, Argumentationsmuster der Befragten erweisen. Übergreifen diese die einzelnen Anwendungssettings – sowohl im Hinblick auf die Bewertung des eigenen als auch anderer Anwendungsbereiche – findet sich, im Vergleich, Sicherheit am häufigsten in den Anwendungsbereichen Schule und Behörde, und ist hier zudem auch am stärksten ausgeprägt. In anderen Anwendungssettings werden Sicherheitsargumente demgegenüber von jenen der Bequemlichkeit überlagert. Korrespondiert dies zunächst mit den spezifischen Strategien der Akzeptanzbeschaffung in den jeweiligen Anwendungssettings (vgl. Böger 2012, Kühne/Wehrheim 2013), zeigten die Beobachtungen, dass die Bedeutung der Fingerabdrucktechnologie in den konkreten Anwendungssettings nur selten explizit ausgehandelt wird. Deutete dies daraufhin,

dass sich der Sinn der Technologie also implizit erschließt, wird im folgenden Kapitel der heterogene Sinn der Technologie entlang der „meaning making resources“ (Lemke 1995: 19)[50] aufgeschlüsselt, an denen sich die von den Befragten geäußerten Zwecke festmachen lassen. Diese Herangehensweise eröffnet für die Frage nach der Akzeptanz den Blick auf die Differenziertheit und Relativität der vermeintlich kategorialen Charakteristika der Technologie und distanziert sich so auch von der bereits kritisierten Grundannahme, wonach sich mit den an die Funktionalität der Fingerabdrucktechnologie anschließenden zweckhaften Versprechen (bzw. ihrer Kritik) bereits der Rahmen entfalte, innerhalb dessen sich (nicht-)akzeptierendes Handeln verorten, es sich mithin erklären ließe.

3.1.1 Heterogene Zwecke im sozio-technischen Setting

Mit der Annahme der interpretativen Flexibilität einer Technologie wird insbesondere darauf aufmerksam gemacht, dass Technologien modifizierbar und der vor allem einzelnen Artefakten zugeschriebene Sinn und Zweck mithin wandelbar ist. Das gilt nicht für die Prozesse ihrer Entwicklung, die die Begründer dieses Konzeptes insbesondere in den Blick nehmen (vgl. Pinch/Bjiker 1984), sondern auch für die Nutzungszusammenhänge, in denen Technologien zur Anwendung gebracht und fortlaufend interpretiert, angeeignet und mitunter auch manipuliert werden. So bestimmt sich die Wahrnehmung der Fingerabdrucktechnologie in den jeweiligen Anwendungssettings nicht allein aus ihrer Funktion als einer Technik der Authentifizierung heraus und auch eine ihr zugeschriebene Nützlichkeit ist nicht immer auch auf die Technologie selbst gerichtet. Vielmehr stellt sich der Sinn der Technologie häufig erst im jeweiligen sozio-technischen Setting her und mitunter eher implizit in Verfahren, Situationen, und sozio-technischen Gegebenheiten, die den Befragten mitunter auch anderweitig schon bekannt oder vertraut sind, dies teilweise bereits bei der Registrierung, teilweise auch erst im Prozess ihrer Anwendung.

3.1.1.1 Eine bequeme Einrichtung im Alltag: Supermarkt & Videothek

Die mutmaßlich bekanntesten Versprechen der Hersteller und Betreiber biometrischer Technologien richten sich auf die Funktionalität der Authentifizierungstechniken und begründen eine Zweckrationalität, die sich auf folgende kurze Formel bringen lässt: „Für die Nutzer kann

[50] Dazu gehören sprachliche, aber auch nicht sprachliche „conventions of gesture and depiction, the symbolic and functional values of actions“ (ebd.).

Biometrie mehr Komfort und/oder Sicherheit schaffen, denn ‚man hat sich ja immer dabei'" (Büllingen/Hillebrand 2000: 339). Die Zweck-Mittel-Zusammenhänge der biometrischen Versprechen transportieren vor allem im Hinblick auf den Komfortnutzen eine Bedeutung der Technologie, welche sich – als ein ‚komfortables Instrument' – letztlich im Artefakt Fingerabdruckscanner als Kern des Verfahrens zu materialisieren scheint. Eben diese Konnotation, so als ob der Gegenstand eine solche Instrumentalität bereits in sich trüge, spiegelt sich auf den ersten Blick auch in den Argumentationen vieler Befragter wider, wenn diese Erwartungen bequemer Effekte durch die Technologie formulieren. Werden diese etwa darin gesehen, dass sich mit dem Verfahren die in alternativen Möglichkeiten der Zugangskontrolle und des Bezahlens wahrgenommene Komplexität letztlich in einem Finger, *„den man immer dabei hat"* (Marius Tapfer, Vid), auflösen lässt, so veranschaulicht das nachfolgende Zitat einer Videothekenkundin das für die Nutzer mit dem Verfahren verbundene Bequemlichkeitsversprechen:

> „Man kann den Code nicht vergessen, also normalerweise ist das ja sonst mit so 'nem PIN und man hat ja schon relativ viele Karten, die mit irgendeinem PIN funktionieren und die sind ja auch alle andern. Das wär' halt noch ein weiterer PIN, den man vergessen, verwechseln oder verlegen könnte. Das [biometriebasierte Verfahren] ist natürlich auch ein Vorteil, man muss daran nicht mehr denken." (Corinna Meier, Vid)

Diese beispiellose Entlastung aufschlüsselnd ermöglicht das Verfahren Corinna nicht nur eine kognitive Erleichterung – etwa Zahlenkombinationen zu vergegenwärtigen –, es bedeutet auch von Besitz entbunden zu sein, wenn mit der Möglichkeit der Nutzung des Fingerabdruckscanners – zumindest theoretisch – nicht länger Bargeld oder die EC- bzw. Kundenkarte mitgeführt werden müssen. So qualifiziert sich das Fingerabdruckverfahren im Supermarkt und der Videothek vor allem als eine sichere *„Bequemlichkeitslösung"* (Rolf Burger, Sm) – eine Funktionalität, die sich primär aus dem Vergleich mit anderen Technologien ergibt, die ähnliche Zwecke erfüllen. Denn es sind die jeweils vorgefundenen und bislang, mehr oder weniger, bedenkenlos genutzten Verfahren und Techniken, die im jeweiligen Settings „fraglos gegeben" (Schütz 2004: 286) sind, welche dann auch die Nutzungsanweisungen für den Gebrauch der neuartigen Technologie stillschweigend bereitstellen. So bedeutet für die Supermarktkunden das Vorhandensein des Fingerabdruckscanners in erster Linie beim Einkaufen eine weitere, technologisch fortgeschrittene, Bezahlmethode zur Verfügung zu haben, mit der sich der Bezahlvorgang im Vergleich etwa zum vergleichsweise mühevollen Ausstellens eines Schecks – auf vier simple Schritte reduziert:

> „ich leg meinen Finger da drauf, es blinkt grün auf, die Kasse springt auf und der Zettel kommt raus, ne? Früher, wenn ich, mich dran denke, wenn man früher 'n Scheck ausgestellt hat, dann hat man da noch die Nummer eintragen müssen, wo man ihn aus-

> gegeben hat, wie hoch der Betrag war, und hat ihn unterschrieben, man hat ihn gegengezeichnet, das hat alles Zeit in Anspruch genommen.“ (Petra Müller, Sm)

Die Passage illustriert, dass sich die Zuschreibung von Bequemlichkeit nicht allein aus der Bedienung des Fingerabdruckscanners ergibt. Die Praktikabilität des Instruments – im Sinne eines zügigen Bezahlvorganges – betonend, richtet die Befragte ihre Aufmerksamkeit vielmehr auch auf, nur teils technische, Handlungsprozesse, welche mit dem neuen Verfahren resp. dem eingesetzten Instrument eine Veränderung erfahren. Beschleunigt sich mit dem Fingerabdruckverfahren nicht nur das eigene, sondern ebenfalls das Handeln der Kassierer im Supermarkt, so gilt die Technologie deshalb als bequem, weil sich mit ihr letztlich der gesamte Bezahlvorgang verkürzt. Unter techniksoziologischen Gesichtspunkten konstituiert sich die Bequemlichkeitsbedeutung folglich aus der Perspektive des technischen (Nutzungs-)Handelns der Befragten, die sich, aus dem „verteilten Handeln“ (Rammert/Schulz-Schaeffer 2002: 42ff.), das heißt einem Zusammenwirken unterschiedlicher technischer Instanzen – zum Beispiel dem Kassensystem – und menschlicher Akteure, ergibt. Die neue Technik hat hier einen wesentlich instrumentellen Charakter und ebenso wie Technik ‚von früher‘ keine besondere Aufmerksamkeit mehr im Alltag erlangt, verschwindet vor diesem Vergleichshintergrund die Bedeutung des Verfahrens dann auch in den bekannten Routinen des Einkaufens. Denn wenn den Befragten das Fingerabdruckverfahren etwa als praktischer als die Mitnahme von Bargeld erscheint oder vom Erinnern des PIN-Codes der EC-Karte entlastet, ist das Verfahren gleichermaßen *„normal“* (Erika Hundt, Sm) und für die befragten Nutzer ein schlichtes Mittel zum Zweck, weil es dann egal ist, *„ob man dann mit Karte bezahlt, oder mit Fingerprint. Ja, ist dann im Grund genommen für mich dasselbe gewesen.“* (Petra Müller, Sm) Das Verfahren wird in diesen Anwendungssettings dann als ein passives Werkzeug erfahren, das gehandhabt und genutzt wird.

Ergibt sich die dem Verfahren zugeschriebene Nützlichkeit folglich aus einer spezifischen technisch-sozialen Einbettung im jeweiligen Setting, das heißt den heterogenen Elementen und Prozessen, die seinen spezifischen Wirkungszusammenhang bilden, dann erweist sich der bequeme Nutzen für die Befragten in der Videothek vor allem als eine Frage der Praktikabilität eines durch beinahe komplette Automatisierung charakterisierten Anwendungssettings, in dem der Fingerabdruck selbst eher nachrangig ist, wie etwa der Nutzer Max Schaf (Vid) ausführt:

> „Nee, also dieser Fingerabdruckscan hat mich eigentlich nich‘ so richtig berührt, sag ich mal so, also es war halt so, ob ich dann nur, ob ich dann nur mir‘n PIN ausgedacht hätte, weil bei den anderen Automaten weiß man ja, is‘ es ja meistens so, dass man einen PIN eingeben muss. Ob ich mir dann nun ‘n PIN hätte ausdenken müssen oder halt wie in

> der [Bibliothek] ‘n Passwort, das ich da hätte eingeben müssen oder ob mein Fingerabdruck halt abgeben, eintippen, eingeben musste, war für mich eigentlich kein Unterschied. Also machte halt vom Gebrauchsgefühl her keinen großen Unterschied und das war halt einfach so, dass ich’s prinzipiell aber irgendwie natürlich irgendwie was, was Neues war, was Interessantes war, glaub ich, denk ich mal wirklich, aber es war jetzt nichts, was jetzt irgendwie man so als jetzt irgendwie was Besonderes wahrgenommen hat. Also ich nich‘. Das war halt irgendwie ok, das war ‘ne neue Eingabemethode, es war praktisch, dass man sich da nich‘ noch’n PIN ausdenken muss und noch irgendwie ‘ne Nummer im Kopf haben muss. Aber es war jetzt irgendwie, ich hab‘s halt irgendwie so gedanklich eben mit PIN oder Passwort gleichgesetzt. So, also es war für mich nichts anderes.“

Wie in dieser Passage deutlich wird, geht für Max das *„Neue“* des Verfahrens nicht zwangsläufig mit einer Erfahrung des „Neuartigen“ (Schütz/Luckmann 2003: 204) einher. Denn auch wenn er an dieser Stelle des Interviews eine emotionale Erfahrung bei der Nutzung der Technologie reproduziert, in der sich die Verbindung des *„Neuen“* mit dem *„Interessanten“* als ein Hinweis darauf lesen ließe, dass dem Verfahren etwas Besonderes anhaftet, referenziert er mit dem *„Gebrauchsgefühl“* gerade das ‚Übliche‘ seines Anwendungssettings: die Notwendigkeit von Zugangsverfahren bei automatisierten Leihvorgängen in einem in der Regel von persönlich anwesenden Mitarbeitern befreiten Setting. Mit diesen „automatischen Erwartungen“ (Schütz/Luckmann 2003: 260) fügt sich das neue Verfahren als ein kommodes, das heißt passendes Instrument (der Authentifizierung) in das Setting ein. Zugangsbarrieren, wie etwa der PIN, die Authentifizierung ermöglichen, haben sich hier bereits so weit zu einem selbstverständlichen Muster abgeschliffen, dass dann auch die Benutzung seines Fingerabdrucks zur Authentifizierung in der Videothek „*nich‘ so richtig berührt“*. In diesem Zusammenhang deuten auch andere Nutzer an, dass das Fingerabdrucksystem, weil es *„so cyber-mäßig“* (Katrin Milcher, Vid) oder auch *„unnötig futuristisch“* (Florian Grippe, Vid) zwar nicht so recht in das „Zeichensystem“ (Schütz/Luckmann 2003: 645ff.) Videothek als einem Freizeitzusammenhang passen mag, sie es gleichwohl als Bestandteil eines sich immer wieder technologisch wandelnden Alltagssettings verstehen, in dem automatisierte Bezahl- oder Zugangsverfahren dann auch Ausdruck legitimer Kontrollinteressen sind. So verweist etwa Herr Borowski, registrierter Nutzer der Automatenvideothek auf bereits aus traditionellen Videotheken bekannte Anmeldungsprozedere und Authentifizierungsprozesse, etwa basierend auf personalisierten Kundenkarten:

> „Naja, wenn man irgendwie so da, was weiß ich, jetzt in ‘ne Videothek geht, muss man sich auch anmelden (Interviewer [I]: Ja). Kriegst du ‘n Ausweis, dann werden die Daten aufgenommen (I: Ja). Mit Fingerabdruck, naja ok, meine Güte. Hab‘ ich auch noch nich‘ erlebt, aber ((lacht)) wenn sie das so wollen, dann sollen sie das kriegen, ja.“

Weil dann auch diese Mitgliedschaftsvoraussetzung auf die spezifische Funktionalität von Automatenvideotheken übertragen wird, welche im 24-Stunden-Betrieb ohne Servicepersonal, das die *„Identität klären kann“* (Karsten Gald, Vid), funktionieren, ist es für die Nutzer nicht nur naheliegend, dass diese eine Form der Identitätskontrolle benötigen, sondern auch, dass diese fraglos einer technischen Umsetzung bedarf:

> „Ich meine, ich kann das natürlich nachvollziehen, irgendwo, weil man halt natürlich gerade jetzt bei irgendwo da jetzt kein direkter Kundenkontakt, der zweifelsfrei die Identität irgendwo klären kann. Kann ich schon nachvollziehen, dass es nötig ist, die Identität des, der der ausleihenden Person zweifelsfrei zu klären.“ (Karsten Gald, Vid)

Dass mit dem Verfahren die direkte Kommunikation zwischen Nutzer und Betreiber ersetzt wird, liegt für die Befragten in deren beiderseitigem Interesse: Rund um die Uhr DVDs ausleihen zu können findet seine Entsprechung in dem vorgestellten Interesse des Betreibers darin, auch in Abwesenheit Gewissheit über die Identität und mithin Zugangsberechtigung seiner Kunden zum DVD-Ausgabeautomaten zu erlangen. Wird insofern das vermutete Kontrollmotiv des Betreibers der Videothek als ein aus der Automatisierung heraus natürliches anerkannt, weil es *„nachvollziehbar“* erscheint, erweist sich die Identitätsüberprüfung als typischer Bestandteil des Settings und die an dieser Stelle unterstellte „Reziprozität der Motive“ (Schütz/Luckmann 2003: 568) als exemplarisch für die Selbstverständlichkeit, mit der sich die Nutzer hier dem Verfahren zuwenden. In dem Maße also, wie Techniken selbst die Tendenz zur Gewohnheitsbildung beinhalten (vgl. Rammert 1988: 174), scheint auch das Element Fingerabdruckabgleich in den bekannten Ablaufprozessen und, im Fall der Videothek, im Bedienen einer größeren Maschinerie zu verschwinden. Denn gerade dieses Setting macht deutlich, dass in Bezug auf den Zusammenhang zwischen Nutzung und Objekt, wie etwa Beck (1997: 190) anmerkt, „die für die Analyse zu ziehenden Grenzen zwischen Objekt und Nutzer […] nicht einfach mit der Außenhaut des jeweiligen technischen Objektes resp. des humanen Subjektes zusammen[fallen].“ In einem komplett automatisierten Anwendungszusammenhang wie der Videothek entfaltet sich der bequeme Alltagsnutzen nämlich erst im reibungslosen Umgang mit der gesamten Maschinerie DVD-Automat, in welche das biometrische Verfahren der Authentifizierung eingebettet ist:

> „Sag ma‘, dass is‘ halt für jedermann ‘ne Sache, ohne dass man da großartig drüber nachdenken muss (I: Ja). Also find ich, ich find‘s nicht schlecht. Es geht auch relativ schnell also, ich mein‘, Karte durchziehen, Finger einmal rauflegen und schon is‘ man im Menü drin, also es dauert keine halbe Minute, denn kann man halt schon Filme ausleihen.“ (Julia Franke, Vid)

Obzwar die Maschinerie die Bedienung des Fingerabdruckscanners gleichsam voraussetzt, verweist der von Julia formulierte Bequemlichkeits-Dreiklang auf ein komplexes Technik-

netzwerk, das es zu bedienen gilt. Wie die Nutzerin hervorhebt, bedarf es für diese Bedienung gleichwohl keinerlei spezifischer Kompetenzen. Als Sache für *„Jedermann“* gilt sie leicht erlernbar. Das Vorhandensein des Fingerabdruckverfahrens selbst ist Teil der Notwendigkeit der Umstände, die ein solch automatisiertes Setting bereitstellt und seine Nutzung ist inkorporiert in die eigentlichen Zwecke, die sich an das Setting knüpfen: rund um die Uhr DVDs ausleihen zu können. Hierfür ist das Verfahren eher sekundär, sein Vorhandensein wird vielmehr gefällig hingenommen. Die Nachrangigkeit der Technologie zeigt sich auch darin, dass diese offenbar auch gegenüber anderen Personen keine besondere Betonung erfährt, wie eine andere Nutzerin erklärt:

> „Ich empfehl‘ die [Videothek] schon, weil das natürlich, wie gesagt, weil man rund um die Uhr die Möglichkeit hat da Filme zu holen oder auch Filme hinzubringen. Deswegen sag ich natürlich schon: ‚Hier, da vorne is‘ sie und total praktisch‘. Da sprech‘ ich aber nich‘ über den Fingerabdruck.“ (Katrin Milcher, Vid)

Steht insofern stattdessen die Praktikabilität des gesamten Settings für die Nutzer im Vordergrund, werden Vorteile, die das Fingerabdruckverfahren nahelegen könnte, auch eher im Kontext einer allgemeinen Automatisierung betrachtet, etwa, dass Filmvorlieben anonym bleiben statt wie in den traditionellen Videotheken im Austausch mit Mitarbeitern *„entblößt“* (Katrin Milcher, Vid) zu werden. Dabei handelt es sich allerdings um Sekundäreffekte, das heißt um Vorteile, die die Videothekennutzer erst nach einiger Zeit für sich entdecken, wenn sie wahrnehmen, dass die Gebrauchsweise, zumindest theoretisch, auf die Mittel zurückwirkt:

> „Ja gut, ich meine, es is‘ natürlich halt bezüglich, halt der Filme, die man auswählt ‘ne größere Anonymität. Es is‘ nich‘ so, dass ich diese, dass ich sie brauchen würde, also für mich sind es dann tatsächlich eher die praktischen Belange, die da den Ausschlag geben, aber es is‘ natürlich klar, selbstverständlich mit ‘ner größeren Anonymität verbunden.“ (Karsten Gald, Vid)

Es zeigen sich in diesen Settings also Handlungsorientierungen, die sich, erstens, mitunter nur indirekt auf das Verfahren beziehen und, zweitens, im Umgang mit der Technik kaum je über technisch-funktionale Gebrauchserwartungen hinausweisen.

3.1.1.2 Ein Kontroll- und Sicherheitsinstrumentarium: Arztpraxis & Schule

Wenn den Nutzern vor dem Hintergrund des Vergleichs mit funktionsgleichen Instrumenten und bekannten Praktiken der Sinn der Technologie als eine augenfällige Aussage, „entgegen“ kommt, um einen Begriff Roland Barthes‘ (1990: 47f.) zu benutzen, dann zeigt sich dies in aller Deutlichkeit auch in der Arztpraxis. Hier ist die Fingerabdrucktechnologie eingebunden

in ein aus vielen Arbeitskontexten bekanntes Verfahren: das Kontrollregime der verbindlichen Zeiterfassung. Obwohl für alle Mitarbeiter verpflichtend, macht es für die Befragten keinen Unterschied, ob die Arbeitszeit über das neue System oder per Stechkarte erfolgt, denn letztere sei *„ja das Gleiche […], nur mit Karte“* (Nicole Kunze, Arzt). Das System dient aus der Perspektive der Befragten primär dazu, innerbetriebliche Gerechtigkeit herzustellen und soll ein bereits etabliertes Regime – die, aus Sicht einiger Mitarbeiter ungenügend funktionierende flexible Arbeitszeitgestaltung – ersetzen, wie auch der befragte Arzt im Interview erklärt. In anderen Worten verbindet sich mit dem Verfahren der Zweck, informelle Kontrolle zu formalisieren, um zu prüfen *„wer wann wie da is‘ […] kriegt man seine Stunden zusammen“* (Kathleen Häuser, Arzt). Dieses Bedürfnis resultiert, zum einen, daraus, dass die Verantwortlichen, der leitende Arzt, diesem nicht hinreichend nachkommen und es zielt, zum anderen, darauf, daraus mutmaßlich resultierende Betrugsversuche anderer Mitarbeiter zu vereiteln, wie Nicole Kunze (Arzt), zu den Bedingungen der Einführung befragt, ausführt:

> „Also [Name einer Mitarbeiterin] halt, die hat gesagt: ‚Ich finde das gut‘, ich sag, ‚dann stimmt ich da auch zu‘ und [Name einer weiteren weiblichen Person] war eher eine so, die das nich‘ so toll fand, aber da hab‘ ich dann einfach den Mund gehalten und meine Gedanken dazu gemacht, weil sie war ja diejenige, die hier freitags dann nich‘ aufgetaucht is‘, wenn Frau [Name einer Ärztin] frei hatte (I: Ja.). Der Doktor arbeitet freitags sowieso nich‘, Herrn [Name eines Assistenzarztes] dann nur dort, das war dann unser Assistenzarzt. Und dann hat sie sich bei ihm krankgemeldet oder so (I: Ja.). Is‘ aber auch nich‘ zum Arzt gegangen und seitdem müssen wir auch, wenn wir ((betont)) den ersten Tag krank sind, gleich ‘ne Bescheinigung abgeben.“

Das legitime Kontrollinteresse des Vorgesetzten erweist sich insofern auch als ein eigenes und die Kontrolle mittels Zeiterfassung ist dann eine zweifache: sie ermöglicht Übersicht über das eigene Handeln – das man die Stunden *„zusammenkriegt“* – und zugleich eine Kontrolle über jenes suspekter Anderer, die zudem für eher unbeliebte Kontrollmaßnahmen verantwortlich gemacht werden. Für die konkrete Umsetzung der Kontrolle stellt gleichwohl das Fingerabdruckverfahren keine notwendige Voraussetzung dar.

In den Schulen zeigt sich diese doppelte Kontrollrichtung ebenfalls und auch hier ist das Verfahren mitunter nur ein indirekter Mittler. Denn die im vorangegangenen Kapitel formulierte Einsicht, dass sich die funktionelle Wirksamkeit des Verfahrens vielfach erst innerhalb unterschiedlicher technisch-sozialer Konfigurationen abbildet, in die es jeweils eingerichtet ist, erhellt, weshalb auch befragte Eltern in den Schulen von Bequemlichkeitsvorteilen berichten, ohne selbst das Fingerabdruckverfahren zu benutzen. Unter diesen Aspekten können die willkommenen Effekte der Technologie nämlich auch vollständig von der Handhabung gegenständlicher Technik losgelöst sein und es verbinden sich für einzelne Befragte zudem gänzlich

neue Funktionen mit dem Verfahren. Eine Mutter, die im Interview erklärt, dass es für ihren Sohn unumgänglich gewesen sei, das Verfahren in der Schule zu benutzen, weil die Familie nur so die mit dem Familienpass verbundene Vergünstigung des Essenspreises in der Schulmensa in Anspruch nehmen kann, beschreibt, obwohl nach möglichen Nachteilen dieser Bezahlmethode innerhalb des behördlichen Kontrollkontextes befragt, stattdessen die bequemen Vorteile wie folgt:

> „Mm ((ablehnend)). Nö, find‘ ich nicht. Weil, du zahlst halt das Geld auf‘n separates Konto ein, also kann dir schon mal was hinlege, das Geld ((klopft mit den Fingerknöcheln auf den Tisch)), das is‘ dann fürs Essen da und fertig.“ (Sabine Walter, Schul2)

Der an dieser Stelle von Frau Walter hervorgehobene bequeme, das heißt entlastende und handlungserweiternde, Effekt des Verfahrens ergibt sich ausschließlich vor dem Hintergrund des komplexen Verfahrens des Onlinezahlungsverkehrs, in welches das Fingerabdruckverfahren in den Schulen eingebettet ist. Der für sie daraus resultierende Vorteil, die der Familie zur Verfügung stehenden knappen finanziellen Ressourcen damit sicher (online) am Monatsanfang *„hingelegt“* und damit buchstäblich festgelegt zu wissen, ist lediglich „informationstechnisch induziert“ (Hubig 2011: 151), statt gegenständlich gegeben. In diesem Fall generieren sich die bequemen Effekte aus einer „atypischen“ Form der Materialität (Tschida 2014: 222), das heißt aus nicht an vor Ort verfügbaren, sondern aus vielzähligen miteinander verbundenen technischen Komponenten, die als konkrete Erfahrungsobjekte kaum zugänglich werden. Wie bei klassischen Artefakten impliziert aber auch ihre Inkorporation die Möglichkeit unterschiedlicher Aneignungsweisen, woran sich erneut verdeutlichen lässt, wie die vermeintlich eindeutige Zweck-Mittel-Relation der Technologie offen ist für eigenwillige Aneignung.

So ist die Nutzung des Fingerabdruckverfahrens in den Schulen nicht nur an settingspezifische Vorgaben gebunden und die Argumente der Eltern zielen mehrheitlich auch darauf, ihre Kinder mittels dieses Verfahrens vor Risiken im Umgang mit Bargeld zu schützen. Dabei handelt es sich um ein Argument, welches sich auch, ‚in locus parentis‘, im Diskurs über das Verfahren in diesem Setting widerfindet und wie es etwa bei der seiner Bewerbung zu Beginn des Schuljahres im Gymnasium vernommen werden konnte: die Kinder würden das Mittagsgeld auf diese Weise weder verlieren, noch könnte es ihnen entwendet werden. Darüber hinaus wird das Verfahren in diesem Setting auch zum Mittel pädagogischer Kontrollambitionen, die sich gleichwohl erst durch die Einbindung der Technologie in jenes größere Verfahren der Organisation des bargeldlosen Zahlungsverkehrs ergeben, wie eine andere Mutter im Interview erklärt:

> „Das Gute is‘, das haben wir auch vorhin […] diskutiert. Man kann das ja doch sehr beschränken, ja, auf welche Anwendung, also, für welche Anwendung das Kind das praktizieren kann. Eben, ich hab‘ also damals gesagt: ‚keine Zwischenverpflegung‘, weil ich eben nich‘ wollte, dass er [ihr Sohn] sich Schokokissen, Laugenchroissants, oder was sie sich da kaufen, kauft. Sondern ich hab‘s auf‘s Mittagessen, hab‘ da irgendwie ‘ne Höchstgrenze, was weiß ich, vier Euro oder so, angegeben, sodass ich also im Prinzip sicher sein konnte, dass das wirklich nur für das Mittagessen verwendet wird.“ (Monika Reckling, Schul1)

Das das Verfahren umgebende Abrechnungssystem gestattet den Eltern folglich eine spezifische Form von technologisch-mediierter Fernkontrolle („remote control“), wie sie etwa von Fotel und Thomsen (2004: 544) am Beispiel der kindlichen Mobilitätsüberwachung untersucht und als Bestandteil einer neuerlichen Restrukturierung kindlicher Freiheitsgrade (vgl. Steeves/Jones 2010: 187) beschrieben wird. So können die Eltern, zum einen, die täglichen Geldausgaben in der Schule limitieren und mithin kontrollieren – ein induzierter bequemer Vorteil, wie er auch in der Argumentation von Frau Walter hervortritt. Über das Treuhandkonto der Stadt wird aber nicht nur das Geld für die jeweiligen Essenskäufe abgebucht, sondern die Eltern können, zum anderen, im Internet neben dem Kontostand auch die jeweiligen Abrechnungen einsehen. Erst mit diesem technischen Zusammenhang wird die Fingerabdrucktechnologie dann auch zum Instrument pädagogischer Kontrolle. Die Zusammenführung dieser unterschiedlichen Effekte des Verfahrens zu einer bequemen Kontrolleinrichtung beschreibt vor allem ein Vater eindrücklich:

> „Ich mein‘, der, der Vorteil des Systems is‘ derjenige, dass man einmal kein Bargeld im größerem Umfang mitnehmen muss und dass die Eltern auch ‘ne Kontrolle haben über das Ausgabeverhalten ihrer Kinder. Wenn ich dem [seinem Sohn] fünf Euro, wenn ich fünf Euro mitgeb‘ oder zehn, kann der auch gegenüber beim [Discounter] sich die Chips und des Cola kaufe, was er liebend gern machen würde. Und so is‘ es also zweckgebunden. Und ich kann aber auch die Ausgaben begrenzen, dadurch, dass ich sag, er kann am Kiosk halt nur für zwei Euro einkaufen am Tag und kann nicht fünf Milchschnitten essen und‘s Vesperbrot wieder mit nach Hause bringen. Also von daher find ich das System, also, das sind die zwei Vorteile für mich.“ (Wolfgang Flieger, Schul1)

In diesem Fall überwiegen die elterlichen Vorteile – ein Vorteil für den Sohn, *„zwei für mich“* – jene, die den Schülern mit dem Verfahren an die Hand gegeben werden und die offenbar auch gegen den Widerstand des eigenen Kindes, gleichwohl in seinem Interesse, durchgesetzt werden. Der spezifische Vorteil liegt dann darin, dass das Fingerabdruckverfahren den Eltern nicht nur gestattet das tägliche Geldausgabeverhalten, sondern auch die möglicherweise schlechten Essgewohnheiten ihrer Kinder zu reglementieren, da die detaillierten Abrechnungen Aufschluss darüber geben, wo und damit nicht nur ob, sondern auch welche Mahlzeiten die Kinder eingenommen haben. Um diese vor ihren eigenen Fehlentscheidungen für vergleichsweise ungesundes Essen zu schützen, erlangen sie auf die Weise Gewissheit

darüber, dass die Kinder tatsächlich die Mensa nutzen, statt beim „*Döner oder Hallo Pizza oder McDonalds"* (Monika Reckling, Schul1) zu Mittag zu essen.

3.1.1.3 Ein bürokratisches Sicherheitsmerkmal: Einwohnermeldeamt

Seltener als ein konkretes praktisches Verfahren erscheint die Fingerabdrucktechnologie unter Sicherheits- und Kontrollaspekten demgegenüber in der Behörde. Im Mittelpunkt steht vielmehr die Wahrnehmung des Fingerabdrucks selbst als ein Sicherheitsmerkmal, das geeignet scheint, die Fälschungssicherheit der persönlichen Identitätspapiere zu erhöhen. Denn obzwar Ausweispapiere bereits biometrische Marker enthalten, identifiziere der Fingerabdruck aus Sicht aller Befragten eben *„mehr als jetzt das Foto"* (Anita Kohlberg, Einwo). Seine Bedeutung für Identitätsfeststellverfahren liegt, wie der nachfolgend zitierte Befragte erklärt, gerade in einer spezifischen *„Exaktheit"* für die Beschreibung einer Person:

> „Wenn ich sage, der is', hat grüne Augen, blaue Haare und is' 77 Zentimeter groß oder wat weiß ich, dann gut, bei dem Beispiel würde es jetzt wahrscheinlich nur einer sein ((lacht)), aber es würde eben halt nicht exakt den Menschen beschreiben. Und das ist eben halt der große Unterschied. Fingerabdruck hat nur ein Mensch." (Carsten Welzer, Einwo)

Das Körperzeichen Fingerabdruck erscheint im Gegensatz zu einer Beschreibung der Person als sicherer, aufgrund seiner Einzigartigkeit mithin als Quelle einer unmittelbaren und augenblicklichen Wahrheit (vgl. Aas 2006: 154) etwa auch dann, wenn, in den Worten eines Antragstellers für einen neuen Reisepass, beim Grenzübertritt im Zweifel der Fingerabdruck zur *„Gegenprobe [dafür werden könnte], ob ich dann derjenige bin."* (Dietmar Lemke, Einwo). Dieser, zumindest theoretische, Nutzen der Fingerabdruckgabe erhärtet sich für die Befragten dann im Verweis auf die bekannte Kontrolle der Identität durch (grenz-)polizeiliche Akteure, wonach der Abgleich der Fingerabdrücke (nicht nur) in diesem Zusammenhang auf komfortable Weise die Erklärung über Identität ersetzt. Die Befragten gehen davon aus, dass sich auf der Basis des in diesem Sinne informatisierten Körpers Identitätsbehauptungen be- bzw. widerlegen ließen – seien diese nun argumentativer Art oder visueller Natur, wenn es etwa darum geht, einen Identitätsabgleich am optischen Erscheinungsbild vorzunehmen. So führt Dietmar Lemke zur institutionalisierten *„Gegenprobe"* dann weiter aus, dass bereits natürliche äußerliche Veränderungen Zweifel an der Wiederkennbarkeit wecken könnten und so der automatische Abgleich der Fingerabdrücke die nicht nur gebräuchlichste, sondern auch institutionalisierteste Art des Wiedererkennens – dem Gesicht zeigen (vgl. Introna/Wood 2004:

178, vgl. zur Kulturgeschichte des Gesichts McNeill 2003) –, in diesem Fall, buchstäblich obsolet machen könnte:

> „Weil ich bin ja nich‘ verpflichtet, wenn ich irgendwo jetzt hinreisen sollte mit mein‘ Reisepass, dass ich jetzt, und ich lass mir ‘n Bart wachsen, den dann abzuschneiden, wenn ich da über die Grenze möchte. Und da nehm‘ die den Fingerabdruck dann eben für.“ (Dietmar Lemke, Einwo)

Im Zusammenhang mit der bekannten grenzpolizeilichen Kontrolle wird die Relevanz der vorgestellten behördlichen Zwecke dann auch vielfach von der Bedeutung, die die Identitätsdokumente selbst haben, überlagert. Die Aufnahme der Fingerabdruckdaten dient dann etwa dazu, die persönlich wichtigen Ausweispapiere „*korrekt zu haben“* (Hans-Peter Janßen, Einwo). In solcherart Zweckorientierungen dieser Befragten schreibt sich zunächst das „project of legibility“ (Scott 1998: 80) fort – lässt sich doch, wie etwa Valentin Groebner (2004: 162) anmerkt, die Bedeutung der bürokratischen Bescheinigungen persönlicher Details für die Praktiken der Identifizierung und Wiedererkennung darin sehen, dass sie zum Stellvertreter für ein teilhabeberechtigtes politisches Subjekt werden:

> „Kontrolliert wurden und werden in Wahrheit nicht Menschen, sondern ihre Papiere. Und diese erweisen sich dann als echt, wenn es viele (fast) identische davon gibt. Pässe eines Staates sind bis auf einige personenbezogene Details gleich. Und ein Mensch ohne solche Papiere hat große Mühe zu beweisen, wer er ist. Danach wird ‚etwas – [oder] jemand‘ – erst authentisch […] durch die Repliken, die von ihm hergestellt werden.“ (ebd.: 168)

Herr Janßen (Einwo) etwa, der sich für die Aufnahme seiner Fingerabdrücke in den Personalausweis entschieden hat, beschreibt den Erhalt seiner ersten Ausweisdokumente dann auch als Endpunkt eines ‚Werdens‘: *„Jetzt gehörst du zu den Menschen.“* Eine andere Befragte betrachtet, analog dazu, die Aufnahme der Fingerabdrücke in den Personalausweis ebenfalls als konsequente Weiterführung ihres *„administrativen Ich’s“* (Greta Böttcher, Einwo). Erweist sich das eindeutige Identifizieren und Wiedererkennen von Personen für die Befragten als Kern des Gewissheitsversprechens, den sie mit der Technologie verbinden, dann wähnen sich viele der befragten Nutzer mit der Speicherung der Fingerabdrücke im Falle des Verlusts der Ausweispapiere aber auch als persönlich sicherer identifizierbar:

> „Ich seh‘ eigentlich nur ‘n Vorteil für mich, weil, falls es da mal Schwierigkeiten geben sollte, dass der verloren geht, hab‘ ich doch noch ‘ne etwas bessere Grundlage. Ich mein jetzt, falls andere Leute den jetzt benutzen wollen, sag ich mal. Ne, is‘ es für mich doch ‘ne größere Sicherheit, dass da ja nur meine Finger drauf sind.“ (Hans-Peter Janßen, Einwo)

Das Verständnis für die Einführungszwecke wird so auch zum Einverständnis eines legitimen Kontrollmotivs. In diesem Zusammenhang liegt für eine Reihe der Nutzer der Sinn des Fin-

gerabdrucks dann auch darin, die Strafverfolgung zu effektivieren, *„dass gerade da die Einreise von Terroristen oder so gestoppt werden könnte, wenn, wenn auch alle irgendwann seinen Fingerabdruck hinterlegt hätte."* (Anita Kohlberg, Einwo) Wenn damit eine assoziative Passung vor allem im Bezug auf eher abstrakte Einführungsgründe wie der Schutz vor Terrorismus, oder wie andere Befragte betonen, eine staatlich verfolgte Migrationskontrolle und/oder Forderungen der USA etabliert wird, dann gerät der Fingerabdruck zum, über den behördlichen Kontext hergestellten, symbolischen Verweis auf Sicherheitspolitik, ohne dass darin auch automatisch immer eine persönliche Relevanz für die Befragten zum Ausdruck käme. In diesem Punkt erweist sich vor allem die Bedeutung des Fingerabdrucks selbst als ein Vermittlungssymbol, das aufgrund seines kriminalistischen Bedeutungshintergrunds und mithin über Kriminalitätsphänomene den Sicherheitssinn des Verfahrens für die Befragten einholt, und man sie daher zur *„Verbrecherverfolgung […] ruhig nutzen [sollte]"* (ebd.). In diesem Zusammenhang konstatieren Lianos und Douglas (2000: 113f.), dass Maßnahmen der Kriminalprävention regelmäßig zu „reminders of dangerousness" werden, was sich dann auch darin zeigt, dass selbst ausdrücklich kritischen Befragten, wie etwa dem 77-jährigen Herrn Petersen (Einwo) das Fingerabdruckverfahren als legitime polizeiliche Sicherheitsmaßnahme gilt, denn *„in der Kriminalität is' natürlich das A und O"* und es fungiert dann auch regelmäßig als Hinweis darauf, dass potentiell Gefahr droht, weil sich

> „alles geändert [hat], glaub ich jetzt, und auch dieses, wir haben ja zu viele Menschen, die unterwegs sind und reisen. Der eine hier und der andere da, ja Gott. Das muss doch schon erweitert werden." (Greta Böttcher, Einwo)

Mit dem Angebot der Fingerabdruckgabe wird der potentielle Nutzer, in anderen Worten, auch in den Zustand versetzt, die omnipräsente Wahrscheinlichkeit von Viktimisierung selbst zu erfahren (vgl. Lianos/Douglas ebd.). So thematisieren eine Reihe von Befragten in der Einwohnermeldebehörde dann auch Situationen der Unsicherheit und des Zweifels, in denen Identitätsnarrative aus ihrer Sicht von vornherein versagen müssen. Seien diese, wie etwa schwere Flugzeugunglücke, gleichwohl noch so unwahrscheinlich, sehen sie, etwa das Ehepaar Janßen (Einwo), in der Speicherung der Fingerabdrücke in den Ausweispapieren in dem Maße eine Sicherheit in diesen so genannten Notfällen, wie über die eindeutige Zuordnung der Abdrücke etwa auch die postmortale Identifizierung von Verunglückten ermöglicht werde:

> Hans-Peter Janßen: „Es ist ja schon vorgekommen, dass, wir sind ja nun Vielflieger, dass, ich sag das mal ganz grob, man wird zerstückelt, und dann findet man da nun so was, und denn"
> Gudrun Janßen ((fällt ins Wort): „Und denn sind Sie froh, dass Sie wissen, dass derjenige auch wirklich da drin war."

In dieser Hinsicht von der Relevanz situationsspezifischer Risiken zu sprechen, bedeutet, dass Hinweisreize für diverse Unsicherheiten, die über Technologien vermittelt werden, zu Bedingungen der Akzeptanz geraten können. Denn die Sicherheitsrisiken, denen die Integration der Fingerabdrücke in die Ausweispapiere begegnen soll und die sich, analog zu den Einführungsbegründungen, auch entlang medial präsenter Narrative wie des „Identitätsdiebstahls" generieren – das, wie Cole und Pontell (2006: 129) herausgearbeitet haben, wiederum selbst Verbindungen mit allgemeinen Kriminalitätskategorien vermittelt –, beanspruchen auch Geltung unabhängig faktischer Relevanz. Die 21-jährige Susanne Jeske (Einwo) etwa verknüpft, stellvertretend für viele Befragte, die Relevanz der Erfassung von biometrischen Daten sowohl mit den Anschlägen vom 11. September 2001 als auch mit der Möglichkeit einer missbräuchlichen Verwendung verloren gegangener Ausweisdokumente, obwohl sie selbst, wie sie im Interview erklärt, *„gar nicht der Typ"* sei, *„der irgendwas verliert, sag ich mal"*. Es ist vielmehr der Sicherheitswert, der sich für sie mit dem Fingerabdruck verbindet, der ihr ausdrückliches Einverständnis begründet:

> „Da is' 'n Bild drinne, aber trotzdem, die Sicherheit geht ja denn natürlich auch vor und auch mit den Anschlägen is' das natürlich sicherer, weil ich sag mal, diese ganzen Filme, die's gibt, da haben die alle gefälschte Ausweise und Reisepässe, fünf Stück."

Interessant an dieser Passage ist, zum einen, die Überzeugtheit, mit der Frau Jeske das Sicherheitsargument verteidigt und, zum anderen, die Quelle, aus der sie die Gewissheit von Unsicherheit schöpft. Werden hier aktuelle Sicherheitsdiskurse mit fiktionalen Darstellungen vermischt, lässt sich darin mit Garland (2001: 147) auch eine kulturelle Überformung von Kriminalität entdecken, denn „to talk about an ‚experience of crime' in this way is to talk about the meaning that crime takes on for a particular culture at a particular time." In der Verknüpfung von Sicherheitszwecken, katastrophalen Szenarien und traditionell-kriminalistischen Zwecken der Technologie werden in gleichem Maße Vorstellungen von Unsicherheit hervorgebracht, wie sie auch definieren, wem die ‚Abwehr' gelten sollten. Die 45-jährige Sybille Brandt (Einwo) etwa erklärt sich die neuerliche Fingerabdruckabdruckgabe in der Einwohnermeldebehörde dann unter anderem damit, *„dass die keine Terroristen haben wollen, die Amis jetzt."* So bringt der symbolische Wert der Fingerabdrucktechnologie gleichsam Normativität hervor: Befragte, die mit der Aufnahme der Fingerabdrücke die Sicherheit der persönlichen Ausweispapiere gesichert sehen, argumentieren dann auch, dass verschiedenste Personenkategorien *„Schummler oder weiß der Henker was"* (Veronika Oppermann, Einwo), *„Betrüger"* (Rüdiger Oppermann, Einwo) oder *„Straftäter"* (Susanne Jeske, Einwo) schlicht darauf aus seien, sich fremde Identitätsdokumente anzueignen. Die mitunter in diesen Vorstel-

lungen der eigenen Fingerdruckabgabe zum Ausdruck kommenden kriminalpräventiven Erwartungen finden ihre Entsprechung dann auch in der Vorstellung einiger Befragter, welche davon ausgehen, dass der Fingerabdruck in zentralen Datenbanken gespeichert wird, auf die polizeiliche Behörden Zugriff haben.

3.1.2 Eine ambivalente Technologie

Die biometrischen Anwendungssettings kennzeichnet folglich nicht nur eine Flexibilität ihrer Anwendungsbereiche. Die Einsatzmöglichkeiten der Biometrie werden auch als ambivalent erfahren. In den heterogenen Zwecken deuteten sich die durchaus positiv bewerten Zwecke bereits an. Weil man den *„unvergleichlichen“* (Erika Hundt, Sm), das heißt individuellen, Finger ja gleichsam immer dabei hat, erscheint das Verfahren auch im Supermarkt sowohl praktischer, als auch im Vergleich zu alternativen Verfahren als sicher(er). Schüler, Supermarkt- und Kunden der Videothek gleichermaßen sehen sich so vor einem Verlust mitgeführter Zahlungsmittel oder dem Ausspähen etwa des PIN-Code der EC-Karte geschützt und keine andere Person kann etwa fälschlicherweise Filme auf den eigenen Namen ausleihen – etwa wenn, wie ein Nutzer erklärt, die komplementär eingerichteten Sicherheitsmechanismen der Maschinerie Videothek versagen sollten:

> „is ‘ne sichere Sache, falls ich mal meine Karte verliere und irgendjemand mit der Karte da in diese Videothek hinein möchte (I: Ja), hat er zwar die Chance, in die äußere Tür oder die äußerste Tür zu öffnen (I: Ja), aber nich‘ in die Maschinen einzudringen. Ne, er kann zwar die Karte durchziehen, könnte denn mein Guthaben aufladen (I: Ja), das geht ohne Fingerabdruck, aber alles andere, da wär‘ der Fingerabdruck notwendig.“ (Rainer Tapfer, Vid)

Sicherheitsargumentation beziehen sich vor allem auf eine hohe technische Verlässlichkeit, durch die sich das Verfahren für die Mehrheit der Interviewten auszeichnet. Die Technologie ist aus ihrer Sicht in der Lage, Identitäten anhand der Merkmale des Fingerabdrucks zu verifizieren, aber auch zu identifizieren. Anders als die Ausweispapiere, die verloren gehen können, erscheint der Fingerabdruck als ein beständiger Beweis resp. Gegenbeweis für Identitätsbehauptungen, wie etwa Herr Oppermann (Einwo) erklärt:

> „Ja. Wir haben uns überlegt, was, was könnte da denn für‘n Missbrauch erstmal, wenn, mit, mit getrieben werden? Und eigentlich haben wir nur gesagt: Ja, wenn unsere Personalausweise wegkommen, wir, sieht man ja mal so, Gangsterfilme, wo der denn so in so‘n Ausweis denn sein Lichtbild so reinklebt und denn ‘ne Folie wieder rüber, also, ne? ((schmunzelt)) Und so. Und denn is‘ ja immer noch den Fingerabdruck, den kann er ja dann nicht fälschen, dieser Gangster sag ich mal.“

Der Fingerabdruck gilt als einmalig und unveränderlich und daher auch nicht fälschbar. Als ein unverwechselbares körperliches Merkmal fungiert er für die Befragten wie ein unsichtbarer körpereigener ‚Schlüssel', der gerade dadurch Schutz garantiert, dass er für andere Personen, und etwa gegenüber einem ausspähbaren Pin der EC-Karte oder dem Gesicht, unsichtbar bleibt. Dieses Uneinsehbare beschreibt, stellvertretend für andere Befragte, ein Supermarktkunde dann auch sehr anschaulich: *„beim Fingerabdruck steht nichts dabei, und selbst wenn, wenn ich meine Finger so hochhalte, wer kann meinen Fingerabdruck erkennen, niemand!"* (Rolf Burger, Sm). Nun gilt aber nicht nur der Fingerabdruck für andere Personen kaum in Gänze sichtbar, sondern auch die Informationen, die dieser in sich trägt – und die ihn als Sicherheitsmerkmal qualifizieren –, erscheinen den Befragten selbst als unzugänglich. Anders als die von ihnen als für durch Interaktionspartner *„erkennbar"* (Karsten Gald, Vid) und *„beschreibbar"* (Susanne Jeske, Einwo) charakterisierten äußerlichen persönlichen Informationen, wie etwa die Augen- oder Haarfarbe, wird der Fingerabdruck als ein Datum wahrgenommen, dem seine Informationen nur entrungen werden können, wenn er demgegenüber *„gelesen"* (Karsten Gald, Vid; Susanne Jeske, Einwo) wird. Der Fingerabdruck erscheint folglich als eine natürliche Chiffre, das heißt als ein individuelles Zeichen, das sich nicht nur selbst ‚exakt' beschreibt, sondern zudem in verschlüsselter Form Informationen über seinen Träger bereithält. Anders als der PIN-Code der EC-Karte kann dieser nicht ausgespäht oder etwa wie eine Stempelkarte weitergegeben werden. Stehen die Informationen des Fingerabdrucks folglich in einem Übersetzungsverhältnis, erwächst gerade daraus seine Sicherheitsbedeutung, was – wohl am deutlichsten in Bezug auf das behördliche Anwendungssetting – in eben jenen informationstechnisch anmutenden Analogien des Lesens, Auslesens oder, wie in der nachfolgenden Passage aus einem Interview mit einem Befragten aus dem Behördensettings deutlich wird, im Begriff der *„Verschlüsselung"* seinen Ausdruck findet:

> „Es is' natürlich 'ne, gewissermaßen auch 'ne, 'ne Verschlüsselung oder so. Das heißt also, ich, also, es is' ein, ein Code eigentlich. Ne? Dass man da so, nicht genau sehen kann, woran, also was is' jetzt besonders an meinem Fingerabdruck und ganz da so. Da können Fachleute wahrscheinlich sagen, ‚Ja, diese Kurve hier ist sehr selten' oder was ((schmunzelt)), aber das is' letztlich was, wo's dann einfach nur um Verschiedenheit geht und nicht, dass man das beeinflussen kann oder dass man damit was anfangen kann, so." (Stephan Löw, Einwo)

Sind die *„Besonderheiten"* des Fingerabdrucks folglich nur durch Experten entziffer- und damit lesbar, dann erweist sich die Sicherheitsbedeutung der Technologie für die Nutzer bereits in einer analogen „Informatisierung des Körpers" (vgl. van der Ploeg 2003b: 58): Der sich (im zeitlichen Verlauf) ändernde Körper ist, zum einen, über den demgegenüber stabilen *„Code"* Fingerabdruck ausschließlich einer technisierten, das heißt methodischen und zielge-

richteten, mithin professionalisierten Form der Expertise zugänglich. Mithilfe neuer Informationstechnologien wird dieser flüchtige, sich zudem (im Raum) bewegende Körper, zum anderen, fixierbar.

Die Einführung neuer Technologien bringt für die Befragten aber nicht nur Sicherheitsgewinne, sondern stets das Risiko ihres Missbrauchs mit sich: Thematisiert werden Szenarien, wie sie etwa in der kritischen Literatur zur biometrischen Identifizierung weithin unter dem Begriff des „function creep“ (vgl. Mordini 2009: 294ff.) – der zweckentfremdenden Verwendung von Daten – gefasst werden, aber auch qualitativ neue Formen der Kriminalität. So kann, den Befragten zufolge, Biometrie nicht nur eigenes Handeln erleichtern oder unerwünschte Handlungen verhindern, sondern letztere auch erst ermöglichen. In den Schulen etwa fürchten Eltern, dass die Nutzung des Verfahrens die Schüler zwar vor einem Diebstahl des Mittagsgeldes schütze, gleichwohl mit dem Verfahren zum Kauf weiterer Mittagessen erpresst werden könnten. Für den behördlichen Anwendungsbereich wiederum argwöhnen die Befragten, dass die Integration der Fingerabdrücke in die Ausweispapiere es Personen geradezu erleichtern könnte, mit den gestohlenen Papieren ihre wahre Identität zu verbergen. Das Sicherheitsversprechen des Verfahrens wird dann mitunter als ein vorläufiges ausgewiesen, ist doch seine Überwindung immerhin vorstellbar. Eine Rentnerin, die sich gemeinsam mit ihrem Ehemann für die Speicherung der Fingerabdrücke in die Personalausweise entschied, mutmaßt etwa:

> „Vielleicht spornt man sie auch manchmal damit an ((schmunzelt)) durch mehr Sicherheit, dass sie da noch mehr ausklügeln, um das trotzdem zu knacken, ne. Kann auch ‘n Ansporn sein.“ (Gudrun Janßen, Einwo)

Jener besondere Einfallsreichtum der auch immer wieder von anderen Befragten erwähnten sogenannten *„findigen Leute“* (Sybille Brandt, Einwo), neu etablierte Sicherheitsmechanismen zu umgehen, erschöpft sich für die Befragten nicht nur darin, die in den Papieren verborgenen Daten zu manipulieren. Umgangen werden könne das automatisierte Identifizierungsprozedere etwa auch durch ein Duplizieren des Abdrucks, theoretisch auch durch ein gewaltsames Entfernen des Fingers. Während hier nun das Risiko des Identitätsdiebstahls in die Frage der Sicherheit der Papiere vor Entwendung und Fälschung selbst gewendet wird – das Narrativ des Identitätsdiebstahls fungiert mithin als infiniter Regress –, bildet sich in den Argumentationen eine grundlegende Vorstellung über das Wirken biometrischer Technologien ab, die Katja Franko Aas (2006: 150, in Anlehnung an Jonathan Simon 1995) als „power without narrative“ charakterisiert. Vor allem im Hinblick auf andere, nicht selbst genutzte, Anwendungsbereiche artikulieren die Interviewten dann eine Unsicherheit angesichts der Möglich-

keit, dass Dritte sich auf diese Weise Zugang zum DVD-Automaten verschaffen oder einkaufen könnten. Für Frau Janßen (Einwo) etwa, die die Fingerabdrücke in ihren Personalausweis aufnehmen ließ, käme der Einsatz dieser beim Einkaufen daher *„überhaupt nich' in Frage"*, denn:

> „Da hätt' ich tatsächlich schon wieder Bedenken, dass das eben nich' mehr sicher genug is', dass da doch irgendwie Schindluder mit getrieben wird, nich'. Dass sie, dass sie das dann doch irgendwie hinkriegen, dass sie die Linien vielleicht so nachmachen. Man weiß ja nich', wo die Technik in fünf, sechs Jahren oder in zehn Jahren is'." (Gudrun Janßen, Einwo)

Können sich neue Unsicherheiten, wie auch bei anderen Technologien, für die Befragten aus den (mitunter zukünftigen) technischen Möglichkeiten selbst ergeben, birgt vor allem die für die automatische Identifizierung notwendige Speicherung das Risiko, dass der digitalisierte Fingerabdruck verlorengehen könnte. Einem Sinnspruch ähnlich formuliert etwa ein Videothekenkunde, stellvertretend für viele Befragte, sein Unbehagen:

> „wenn da aber die Daten dann aber erstmal abgeflossen sind, dann sind sie weg. Und was die kriminellen Energien, die dann dies dann wie auch immer beschaffen, damit anfangen, das is' nachher wieder 'ne ganz andere Geschichte." (Karsten Gald, Vid)

Die Befragten thematisieren folglich nicht nur Befürchtungen hinsichtlich der Praktiken, die persönlichen, zur Identifizierung geeigneten Informationen einer Person zu stehlen, mit dem Ziel, diese missbräuchlich zu verwenden, sondern sie gehen davon aus, dass die persönlichen Daten insgesamt kaum gegen Verlust zu schützen sind:

> „Naja. Ich sag mal so: Man kennt das ja jetzt schon. Man hat jetzt schon 'ne Menge Datenskandale mitgekriegt in letzter Zeit. Es gibt wieder, immer wieder Datenpannen, es gibt Hacker, die sich vielleicht irgendwo einhacken, es muss ja noch nich' mal gewollt sein. Es gibt immer wieder Korruption beim Menschen, das ist einfach so, das heißt, es könnte eben halt auch sein, dass eben einfach mal ein Mitarbeiter Daten kopiert." (Carsten Welzer, Einwo)

Ein Gefühl von Kontrollverlust bezieht sich für die Befragten, zum einen, darauf, dass die Digitalisierung der Daten in sich virtuelle Prozesse und ‚Orte', etwa der Datenverarbeitung und -speicherung, (ver-)birgt, die nicht greifbar, da nicht sichtbar und oder eindeutig lokalisierbar, sind. Sie geben damit ein Unbehagen wieder, das auch die kritische Literatur zum „Verschwinden der Überwachung" angesichts der Digitalisierung und Miniaturisierung bei gleichzeitiger Vervielfältigung und Mobilisierung der Technologien problematisiert (vgl. Murakami Wood 2011, Marx 2002):

> „Und, wo der Fingerabdruck jetzt letztendlich gelandet is', wer am Ende der Strippe dranhängt, kann ich nich' sehen. Also, klar, der Monitor zeigt's an, aber wo die Strippe letztendlich noch hingeht in der Behörde, ich kann das nur hoffen, dass das prak-

> tisch da an dem Tisch bleibt, oder an dem, an dem, ja, in dem, in deren System. Das is‘, dass das System jetzt nich‘ irgendwie, wat weiß ich wohin geht.“ (Christian Zander, Einwo)

In diesem Zusammenhang werden die Möglichkeiten der Überwachung mittels der Fingerabdrucktechnologie dann auch als ein besonderes Risiko vergegenwärtigt und aus Sicht der Befragten könnte nun der Fingerabdruck, zum anderen, bei der Erstellung von Profilen geradezu als Referenzpunkt fungieren und so Zugang zu weiteren Daten ermöglichen, die jedoch für die Fingerabdrucknehmer beziehungsweise (interessierte) ‚Dritte‘ unsichtbar bleiben sollten. Jederzeit offenbar werden könnten so etwa in der Videothek die persönliche Filmhistorie, die individuellen Einkaufsgewohnheiten im Supermarkt oder gar umfangreiche Bewegungsprofile, die sich, in Kombination mit anderen Daten, erstellen ließen:

> „Also, die Kreditkartendaten, das is‘ ja ‘ne Mastercard, das heißt ja nur Mastercard, das is‘ ja weltweit. Wenn du damit irgendwo bezahlst, is‘, weiß jeder weltweit, am 21.11. war ich im Café sowieso. Das is‘ der Hintergrund, und ich denke mal, da jetzt noch ‘n Fingerabdruck dazu geben, das is‘ ja wie ‘ne Spur legen. Glaub ich zumindest. Für mich is‘ das so.“ (Christian Zander, Einwo)

In der festen Annahme von der Einzigartigkeit des Fingerabdrucks wandelt sich für die Befragten das eigentlich sichere, in diesem Sinne Sicherheit gewährleistende, Signum Fingerabdruck in ein Zeichen riskanter Evidenz. Sie bringen dann eine Befürchtung hinsichtlich der Lesbarkeit des Körpers zum Ausdruck, die in der Literatur zu automatisierten Kontrolltechnologien etwa bei Joseph Pugliese (2010: 23) im sprachlichen Bild der In-Geiselhaftnahme des Subjektes durch den Körper aufgeht: „Hostage to the timbre of its voice and the colour of its irises, the body offers itself up despite the subject.“ In diesem Zusammenhang ist es aber nicht nur die körperliche Be-, sondern auch die Verfasstheit der Technologie, die den Interviewten ein Gefühl der Unsicherheit einflößt. Wird der Fingerabdruck zudem im Alltag überall und jederzeit hinterlassen, sei er in den Händen derer, die ihn finden oder, wie einer der nachfolgend zitierten Befragten imaginativ entfaltet, gezielt auf ihn zugreifen, ihn mithin ‚lesen‘ könnten, dann auch geeignet, Zusammenhänge herzustellen oder eben eine *„Spur zu legen“*, die, in den Worten Irma van der Ploegs (1999b: 301), „turn the individual’s body into a witness against themselves“:

> „Irgendwie geht man mal über ’ne Straße oder was weiß ich oder hin und her und tüdelüt und auf einmal is‘ man da in eine Situation eingebettet, wo das so verrückt ist, denn auf einmal sagt man ‚Ja, Sie haben aber da Ihren, da sind Ihre Fingerabdrücke‘, weil ich zwei Tage vorher da am Briefkasten war oder was weiß ich nicht alles. Fantasie. Aber ein ungutes Gefühl auf jeden Fall.“ (Thorsten Hildesheimer, Einwo)

In diesen Schilderungen scheint der Fingerabdruck zudem, einem Artefakt gleich, ein Eigenleben zu führen: er agiert autonom, separiert vom Körper und scheinbar unabhängig vom eigenen Willen. Bereitet die Vorstellung einer solchen Unverfügbarkeit und eigentlich unwahrscheinlichen, weil *„verrückten"* Situation dem Befragten ein *„ungutes Gefühl"*, dann auch deshalb, da ein solche Verselbstständigung des Fingerabdrucks mithin gespenstisch erscheint. Der Fingerabdruck – sowohl der natürliche als auch der digitalisierte – wirkt in dieser Vorstellung nämlich einem Schemen gleich, der, zwar selbst in seiner Gestalt kaum erkennbar, gleichwohl aber potentiell ein Sichtbarkeitsregime etablieren könnte. Den Möglichkeiten sind dabei aus der Sicht der Befragten keine Grenzen gesetzt, denn denkbar erscheint alles:

> „Aber das ist immer so weit gesponnen dann auch, wie ich dann in so meinen Krimis dann auch lesen, es sind manche Sachen utopisch, aber es gibt auch eben Sachen, die können dann eben doch vorkommen. Ja. Dass es dann doch keine Utopie mehr is'. Ne? Das is' vielleicht auch so'n bisschen die Angst, ich weiß es nich', ne?" (Angelika Wilde, Einwo)

Das Mögliche flößt den Befragten vor allem deshalb ein Gefühl der Angst ein, weil es im Bereich des Utopischen immerhin vorstellbar ist. In der Charakterisierung von Sichtbarkeitsregimen beschreiben Leon Hempel, Susanne Krasmann und Ulrich Bröckling (2011: 8) in der Einleitung zum gleichnamigen Sammelband den von den Befragten hier zum Ausdruck gebrachten ‚unheimlichen' Mechanismus: Sichtbarkeitsregime „holen Verborgenes ans Licht oder sorgen dafür, dass es den Blicken entzogen bleibt; sie vergrößern Winzigkeiten oder zoomen Weitentferntes heran und machen es so für regulierende Zugriffe erreichbar." Auf die Aussagen der Befragten zurückgewendet: obwohl sich dem Besitzer des Fingerabdrucks weder seine Informationen erschließen, noch sich der ‚verlorene' Abdruck dem Auge offenbart, folgt er seinem Besitzer wie ein Schatten und ermöglicht, erfasst und gelesen durch den Expertenblick, eine eindeutige Identifikation mit unvorhersehbaren Folgen:

> „Ist ja nich' so die Frage des eindeutigen Identifizierens. Sondern es geht ja, Fingerabdruck is' ja gerade dadurch berühmt geworden, dass alles was man anfässt, auf einen zurückverfolgt werden könnte sozusagen. Das heißt, ich fasse irgend'nen Gegenstand an und es kann zurückverfolgt werden, das war diese, war ich, und das tut man zum Beispiel mit äußerlichen Merkmalen nich', das geht halt nur mit einem Fingerabdruck." (Carsten Welzer, Einwo)

Ist diese Passage ein erneuter Beleg für die zugrundeliegende Idee, dass die Technologie in der Lage ist, eine Person von einer anderen zu unterscheiden und dies unabhängig von Zeit und Raum, dann gehen damit auch jene Befürchtungen einher, dass der hinterlassene Fingerabdruck eine Spur zu seinem Eigentümer liefert. Eben dieser Glaube an die Möglichkeit einer eindeutigen Identifizierung und die Wahrnehmung, keine Kontrolle über die Datenpreisgabe

zu besitzen, vermitteln ein beklemmendes Gefühl. Vergleichbar dem Originalmodell des „gläsernen Homunculus“[51], der den Blick in das Innere des menschlichen Körpers ermöglicht, bringen die Befragten dann Befürchtungen zum Ausdruck, etwa dem Blick des Staates komplett ausgeliefert zu sein:

> „Ok, wir woll‘n da die Grenzen sicherer machen oder so. Anderes wär‘ schlimm, wenn sie den gläsernen, noch mehr den gläsernen Menschen hervorheben woll‘n dadurch. Also mich noch mehr festnageln woll‘n, denk ich. Das würd‘ ich also nich‘ so schön empfinden.“ (Thorsten Hildesheimer, Einwo)

Dieser Interviewauszug steht dann auch exemplarisch für ein regelmäßig von den Befragten geäußertes diffuses, gleichwohl grundlegendes, Unbehagen angesichts der Digitalisierung der Daten, welches mithin nur bildhaft bzw. der Metapher ähnlich vermittelbar scheint: *„Orson Wells, der gläserne Mensch – wie lange hab‘n wir ihn? Wo bin ich überall registriert? Ich weiß es nicht.“* (Thorsten Hildesheimer, Einwo). Ein Gefühl des ‚Un-Heimlichen‘ hinsichtlich dessen, was sich jenseits der Wahrnehmbarkeit abspielt, kann folglich sowohl positiv als auch negativ bewertet werden, wie etwa auch die Untersuchung von Bug und Wagner (2015) zur Akzeptanz von Überwachungstechnologien im Flughafenkontext andeutet: Während die nicht sinnlich nachvollziehbaren Möglichkeiten der Datenverwendung, zum einen, „ein diffuses Gefühl des Beobachtetseins“ (ebd.) auslösen können, kann, zum anderen, die Tatsache, dass Maßnahmen unsichtbar bleiben – hier zum Beispiel, dass der ‚Code‘ Fingerabdruck durch Laien nicht zu entschlüsseln ist – gleichsam ein Indikator für ihre Sicherheitswirkungen sein.

3.1.3 Das Wissen vom Fingerabdruck

Wenn die Interviewten einen Nutzen in der Technologie erkennen, dies zugleich aber die Wahrnehmung von Risiken nicht ausschließt, dann lässt sich dies zunächst darauf zurückführen, dass keiner der Befragten die Validität des Fingerabdruckbeweises selbst in Frage stellt – ob es sich nun um die Spuren handelt, die Menschen auf Gegenständen hinterlassen oder das sogenannte „data-double“ (Haggerty/Ericson 2000: 625), der Referenzfingerabdruck bzw. das Template und letztlich auch alle anderen persönlichen Marker, die in Datenbanken (zu Profi-

[51] Der „gläserne Homunkulus“ ist ein anatomisches Menschenmodell von Franz Tschackert: eine dreidimensionale Figur, die von einer durchsichtigen Kunststoffhülle umgeben, den Blick auf das Skelett und die inneren Organe preisgab (Beier 1990) und 1930 auf der 2. Internationalen Hygiene-Ausstellung im Hygiene-Museum Dresden ausgestellt wurde. Aber schon 1795 erzählt der Schriftsteller Christian Heinrich Spieß (1966) in den „Biographien der Wahnsinnigen“ die Geschichte eines jungen Mannes, der plötzlich glaubt, eine „Brust von Glase“ (54) zu haben. „Der gläserne Ökonom“ (44) fürchtet, dass so nun alle seine Emotionen für seine Umwelt, die ihm buchstäblich ins Herz schauen kann, lesbar seien.

len) zusammengeführt werden. In dieser Ambivalenz zeigt sich damit ein grundlegendes Deutungsmuster, das auf den Glauben der Befragten an die Objektivität der Technologie verweist, das sich in drei, aufeinander verweisende, Elemente aufschlüsseln lässt: es erweist sich, erstens, in der festen Annahme von der Einzigartigkeit des Fingerabdrucks[52] im Sinne einer "natürlichen Wahrheit" (zur „Naturwahrheit" als wissenschaftlicher Leitvorstellung vgl. Daston/Galison 2009) und, zweitens, in einem Glauben an die Autonomie der Daten. Diese erscheinen, analog zur rechnerischen (Gates 2013: 253) und mechanischem Objektivität (vgl. Daston/Galison 2009: 121), aber nicht nur zu jedem Ort übertragbar, sondern die Beweiskraft der Daten entfaltet sich für die Befragten, drittens, vielfach gerade erst im Urteil von geschulten Experten. Dieses Wissen vom Fingerabdruck, das sich in diesem Glauben an die Objektivität ausdrückt, und an das sich Vorstellungen von Funktionalität und potentiellem Wirken der Technologie – gleichermaßen positiv bewertete Folgen, wie auch irritierende Momente – anschließen, fungiert als ein implizites Wissensprogramm. Es soll, in Anlehnung an Candace Slater (2003) und Madeleine Akrich (1992, 1995), als ‚Bio-Skript' bezeichnet werden: eingeschlossen im Bio-Script ist, zum einen, ein Wissen über die menschliche Natur – für Candace Slater (2003: 8) erschließt sich unter diesem Begriff eine spezifische Narration, wie Natur (im Fall ihrer Untersuchung: der Regenwald) selbst repräsentiert wird. Zum anderen inkorporiert es sich daran anschließende Szenarien, Wirkungsweisen und Handlungsrationalitäten. Das Skript deutet also auf eine Objektivierung von Wissen, das sich für die Befragten in der Symbolik des Fingerabdrucks selbst abbildet. Trotz unterschiedlicher Zwecke der Technologie in den untersuchten Anwendungssettings etabliert das Bio-Skript das Gemeinsame im Unterschiedlichen. Im Hinblick auf ein symbolisches, mitunter normatives Moment von Technologien lautet dann auch eine bekannte Einschätzung der Techniksoziologie, dass technische Gegenstände fremdes Wissen, Wollen und Können umfassen, die sich dem Anwender vielleicht nicht erschließen, gleichwohl aber aufdrängen können, sobald er versucht, sich mit der Technik vertraut zu machen (vgl. z.B. Ropohl 2010: 123). Vor allem die kulturalistisch orientierte Technikforschung betont, dass Technik im Verlaufe von „Produktion, Diffusion und Gebrauch" selbst zum „Träger symbolischer Sinncodierungen" werden kann (Hörning 2001: 78). Wendet sich Hörning dabei aber der alltäglichen Praxis der Verwendung materieller Technik zu, lässt sich diese Einsicht mit Norbert Wiener (1989: 138f.) im Hinblick auf die Prägung des Fingerabdruckverfahrens als eine Abstraktion gesellschaftlicher Erfahrung fas-

[52] Wie weit verbreitet diese Annahme ist, zeigt sich dann auch darin, dass etwa in der Gesprächsanalyse die Spezifik institutioneller Interaktionsbedingungen innerhalb eines Settings als „fingerprint" bezeichnet wird (Heritage and Greatbatch 1991: 95f. zit. in Heritage 2004: 225).

sen: Seiner Beobachtung nach ist es nämlich „an interesting reflection that every tool has a genealogy, and that it is descended from the tools by which it has ifself been constructed."

So besitzt das Fingerabdruckverfahren für die Befragten nicht nur eine „Objektivitätsästhetik" (Gates 2013: 243) – vergleichbar den von Kelly Gates thematisierten Bildern, die durch Videoüberwachung produziert werden –, sondern auch eine spezifische Ästhetik der Glaubwürdigkeit, welche sich in einer historischen Traditionslinie des professionalisierten Fingerlesens illustriert:

> „Ich les gerne Krimis. Ich denk' mal so, Fingerabdruck is', jeder hat seinen Fingerabdruck, und das is' ja 'ne ganz, ganz individuelle Geschichte, nich'? Und, die man, denk ich mal, auch nicht verändern kann, abändern kann." (Angelika Wilde, Einwo)

Die Objektivität der Technologie und mit ihr der Vorgang des Fingerabdruckhinterlassens, -findens oder -nehmens ist somit Zeichen für eine Konvention (technischen Handelns), welche für die Befragten vor allem in Kriminalgeschichten abgebildet ist beziehungsweise dort ihre Bestätigung findet, denn *„wenn man das so im Fernsehen sieht, die Krimis und so weiter. Immer erst Finger-, Fingerabdruck"* (Greta Böttcher, Einwo). Die Ursprünge dieses skriptvermittelten Wissens liegen folglich in Fiktionen, genauer gesagt in, in der Regel, durch Fernseh-Formate vermittelten Bildern der polizeilichen, mitunter detektivischen Arbeit, welche jenen unerschütterlichen Objektivitätsglauben – vergleichbar dem „CSI-Effekt" (vgl. z.B. Cole/Dioso-Villa 2009, Tyler 2006)[53] – illustrieren. ‚Krimis' als Sinnbild der Sicherheitsarbeit bilden insofern im wörtlichen Sinn das Storyboard – sie visualisieren das Drehbuch und re-produzieren das Bio-Skript.

Wird die Objektivität der Technologie also nur selten in Frage gestellt, dann bleibt so weiterhin erfolgreich ausgeblendet, dass die Voraussetzung der Individualisierung, die Annahme der Einzigartigkeit des Fingerabdrucks, bislang weder verifiziert noch falsifiziert wurde, noch dass, wie auch der Blick auf die Historie des Verfahrens zeigt, dem Fingerabdruckabgleich Interpretationsleistungen zugrunde liegen (vgl. Cole 2008, 2005, Pugliese 2010), die allerdings im Rahmen der „Verwissenschaftlichung" des polizeilichen Verfahrens zunehmend „vergessen" wurden (Pugliese 2010: 38), *sodass* der Fingerabdruck zum Symbol für Individualität werden konnte. Diese „Geste aus der Vergangenheit" (Reichertz 2014: 117) lässt sich dann auch in den Beurteilungen der Befragten darin identifizieren, dass der Fingerabdruck

[53] Hinter dem Stichwort „CSI-Effekt" – benannt nach der gleichnamigen US-amerikanischen TV-Serie – verbirgt sich eine Diskussion darüber, welche Wirkung der Konsum von Fernsehsendungen über Verbrechensaufklärung auf Vorstellungen von den Möglichkeiten der kriminalistischen Arbeit bzw. auf die Rolle forensischer Beweise hat. Im Besonderen wird dabei im US-amerikanischen Raum dem Einfluss auf die Urteilsfindung von Geschworenen nachgegangen (vgl. z.B. Tyler 2006). Für einen Überblick zum CSI-Effekt in Deutschland sowie Ergebnissen einer ersten qualitativen Studie vgl. Englert (2014).

nicht nur als der *„beste Beweis“* (Greta Böttcher, Einwo) gilt, sondern auch als die bewährteste Identifizierungstechnik, wie ein anderer Befragter erklärt:

> „aber der Fingerabdruck ist ja so weit ausgereift, da er ja bei der Polizei funktioniert, also muss er ja auch so funktionieren. Denk ich mal.“ (Dietmar Lemke, Einwo)

Analog dazu beweist die Vorstellung von der Objektivität der Technologie ihre Gültigkeit im Hinblick auf die praktische Verwendung dann auch in einem hohen Grad an unbefragter Funktionsunterstellung. Auf dieser Ebene lässt sich der Versuch, ein Artefakt vermeintlich ‚sachgemäß‘ zu verwenden, auf eine in die gegenständliche Technik eingeschriebene Bedeutung zurückführen: Vor allem Kunden der Videothek sowie befragte Schüler wenden sich in den Interviews regelmäßig dem faktischen (Nicht-)Funktionieren der gegenständlichen Technik zu und weisen diese dann mitunter auch als unbequem aus. Allerdings stellen für sie jene Widerstände, ebenso wie die Strategien zu ihrer Überwindung, nur selten die dem Verfahren grundsätzlich zugeschriebene Bequemlichkeit in Frage, weil der ‚Fehler‘ in der Regel nicht dem einzelnen technischen Artefakt oder etwa biometrischen System resp. deren Hersteller oder Betreiber zugeschrieben wird, sondern, und dies erweist sich als ein dominantes, die Anwendungssettings übergreifendes Muster der Argumentation, vielmehr im eigenen Bedienhandeln gesucht wird. Er wird etwa dem ungeübten Umgang mit der Technik zugeschrieben, weil *„der Finger nich‘ richtig drauf“* war (Merle Jürgens, Schul1) oder nicht an der richtigen Stelle, denn: *„dann war‘s einmal zu tief unten, zu tief an der Seite, es muss in der Mitte sein.“* (Pascal Pradhan, Schul2). Aber auch körperliche Defizite, zum Beispiel Verletzungen der Fingerkuppe, werden als mutmaßliche Ursachen dafür identifiziert, dass der Scanner den Fingerabdruck nicht *„erkannte“*: *„Und da hab‘ ich gedacht: Hä, hab‘ ich irgendwie ‘ne Narbe am Finger?“* (Katrin Milcher, Vid)

Es ist nun eine etablierte techniksoziologische Einsicht, wie sie etwa Rammert und Schulz-Schaeffer (2002: 12) erneut formulieren, dass sich Technik nicht auf eine passive Objektrolle reduzieren lässt, sondern sich, etwa auf der Ebene der praktischen Nutzung, als durchaus widerspenstig erweisen kann. Und so sind es dann auch jene Umgangsstrategien, zu denen es dann auch gehört, bereits im Vorfeld der Benutzung auf die Textur, zum Beispiel die Unverletztheit der eigenen Finger zu achten – denn *„das reicht dann schon, wenn irgendwie ‘ne kleine, ‘ne kleine Verletzung da is‘“* (Rainer Tapfer, Vid) –, die die Annahme untermauern, dass sich die erwartete Wirkung der Technologie – etwa die Erleichterung und Beschleunigung der Vorgänge – eben nicht (allein) aus einer „Materialität der Form“ (Rammert 2007a: 56) ergibt. Sie ist vielmehr das Resultat von in Gewohnheitshandeln überführten Interaktivitäten, wie sie Rammert und Schulz-Schaeffer (2002: 12) als „situativ gefundene, erprobte und

auf Dauer gestellte und immer wieder aktivierbare Sequenz von Abläufen“ (ebd.) im Umgang mit der Technik beschreiben. Vor allem das Bequemlichkeitsversprechen der Technologie wird dann solange nicht hinreichend fraglich – dass etwa ein Nutzungsabbruch erwogen würde –, wie es den Befragten im Umgang mit dem Fingerabdruckscanner gelingt, die aus ihrer Sicht erforderlichen körperlichen Bewegungsabläufe einzuhalten und zu schematisieren. Die Nutzer nehmen folglich eine Haltung gegenüber dem Handeln des technischen Artefaktes ein, in der das Funktionieren durch Eigenleistung im Rahmen der „medialen Interaktivität“ von Akteur und Technik (ebd.: 20) herzustellen ist. Ein solches an Erfolg bzw. Misserfolg korrigiertes Handeln – in der Terminologie der Akteur-Netzwerk-Theorie, ein Anpassen an das technologische „Designskript“ (Akrich 1992: 206) – bedeutet, etwa zu vergegenwärtigen, dass man nicht *„den falschen Finger nimmt“* (Max Schaf, Vid) oder solange Erfahrungswissen (von taktilen Operationen bis hin zu erinnerndem Handeln) im Umgang mit dem Gerät zu erwerben, bis man *„einfach den Dreh [raus hat]“* (Julia Franke, Vid.). Diese Strategien verdeutlichen überdies, dass für eine Kontrolltechnik gerade auch das Nichtfunktionieren zum wesentlichen Bestandteil ihres Funktionierens gehört. Und so stimmen diese Beobachtungen, dass die Befragten also bei Störungen weniger an der Funktionalität als vielmehr am eigenen Bedienhandeln zweifeln, dann auch überein mit dem aus den Surveillance Studies bekannten Phänomen einer Objektivierung technologisch begründeter Aussagen, sowohl in der Anwendungspraxis als auch im wissenschaftlichen und sicherheitspolitischen Diskurs (Aas 2006: 150, Cole 2006).

3.1.4 Zusammenfassende Überlegungen

Die Fingerabdrucktechnologie lässt sich insofern nicht nur als ein konkretes und im Wortsinn fassbares Erfahrungsobjekt ausweisen. Es ist nicht allein gegenständlich gegeben, sondern zugleich Repräsentation oder wie Stefan Beck (1997: 349 mit Bezug auf Castoriadis 1990) im Hinblick auf die Rolle von Diskursen für den Umgang mit Technik spezifiziert, als ein „imaginäres Konstrukt“ für die Subjekte vorhanden. Als imaginäres Objekt laufen ihm, in Wolfgang Isers Worten (2007: 481), „inaktuelle oder aspekthafte Bilder […] ‚voraus‘“. In diesem Sinne evoziert das Objekt Fingerabdrucktechnologie aber nicht nur Zuschreibungen zur materiell-technischen Funktionalität des Artefakts. Indem es zugleich als Objekt der Vorstellung existiert, werden Gewissheiten über Sinn und Zweck dann auch nicht nur entlang seiner settingspezifischen Nutzungszusammenhänge relevant bzw. durch sie hervorgebracht. Vor- und

Nachteile ‚des' Fingerabdruckverfahrens werden vielmehr auch durch die ihm anhaftenden (fiktiven) Bilder selbst mitkonstituiert.

In diesem Zusammenhang zeigt sich dann auch, dass Akzeptanzbereitschaften auf der Verhaltensebene als auch die ‚guten Gründe', den Fingerabdruck (nicht) zu nutzen, folglich nicht unbedingt auf gesicherten Annahmen und Informationen über die Technik und deren Verwendung beruhen müssen. So machen zwar viele Befragte ihre Visionen der Überwachung an faktischen Beispielen, zum Beispiel an Maßnahmen oder Gesetzeslagen, fest. Gleichwohl gehen sie auch von der zentralen Speicherung ihrer Fingerabdrücke in einer Datei des Einwohnermeldeamtes aus – was bislang nicht der Fall ist, denn sowohl das geänderte Passgesetz als auch das Gesetz über den Personalausweis verbieten ausdrücklich die Speicherung von Fingerabdrücken in zentralen Datenbanken[54].

Medial präsente Narrative, etwa zum „Identitätsdiebstahl", vermitteln sowohl eine Vorstellung von den technischen Möglichkeiten der Nutzung, als auch des Missbrauchs, welche sich für die Interviewten durchaus als ‚faktische Möglichkeiten' darstellen. Im Hinblick auf die mögliche Überwachung, die komplex und uneindeutig scheint, werden diese dann auch weniger analytisch – im Sinne einer Auseinandersetzung mit dem technisch Möglichen –, als vielmehr in symbolischen Referenzen eingeholt: Auf diese Weise wird das Unvertraute ins Vertraute überführt (vgl. Luhmann 2001: 146), etwa das diffuse Unbehagen in Form von „1984" – der Verknüpfung undurchschaubarer Technik mit dem Potential der Kontrolle – oder im Narrativ des „gläsernen Menschen", mithin einer gefühlten „Atmosphäre" (vgl. Anderson 2009) von Überwachung, in der ein solches Unbehagen mitunter nur in Form von Bauchgefühlen und Vermutungen existiert. Die Interviewten rekurrieren folglich auf die gleichen Topoi der unabsehbaren Bedrohung durch totalitäre Macht und technisch realisierte Kontrolle, die sich auch im kritischen Diskurs ausmachen lassen. Vor allem George Orwells „1984" ist wie kein anderes zu einem, dringliche Datensparsamkeit suggerierenden, Synonym für eine dystopische Welt staatlicher Überwachung und bedrohter Privatheit geworden, das spätestens seit 1978 im deutschsprachigen medialen Diskurs für die Idee von Überwachungspraktiken Verwendung (z.B. Der Spiegel 1978) findet und Barnard-Wills (2011) etwa auch für den Mediendiskurs in Großbritannien ausweist.[55] Wie weit diese Verselbstständigung

[54] Gesetz zur Änderung des Passgesetzes und weiterer Vorschriften vom 20.07.2007, BGBl. I: 1566; Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften vom 18.06.2009, BGBl. I: 1346.

[55] In Deutschland findet er zudem seine Referenz im „Big Brother Award", einer ‚Auszeichnung', die seit 2000 jährlich von dem, dem Grundrechts- und Datenschutz verpflichteten, Verein Digitalcourage an zahlreiche Organisationen, Behörden, Unternehmen oder Einzelpersonen vergeben wird, deren Handeln regelmäßig die Privatheit der Bürger bedroht oder die Datensicherheit beeinträchtigt. Auch biometrische Technologien haben in

reicht, zeigt sich dann auch in der mutmaßlichen Verwechslung von Herrn Hildesheimer (Einwo), der anstelle Georg Orwell *„Orson Wells“* als Metapher nutzt, um sein Gefühl gegenüber gegenwärtigen Überwachungstendenzen zu beschreiben.

Vorteile des Verfahrens und Skepsis speisen sich also gleichermaßen aus Fakten wie aus Fiktionen, das heißt Film oder auch Literatur. Man kennt Identitätsdiebstähle nicht nur aus *„Filmen“* (Susanne Jeske, Einwo), den Fingerabdruck aus dem *„Tatort“* (Corinna Meier, Vid) oder den *„alten Kriminalfällen“* (Rüdiger Oppermann, Einwo). Vorstellungen vom Wirken, ebenso wie potentielle Risiken der Technologie sind auf engste verknüpft mit dem Technoimaginären: In Bezugnahmen auf *„Julius Verne“* (ebd.) oder *„futuristische Kriminalfilme“* (Wolfgang Flieger, Schul1) entfaltet die Technologie dann auch ein faszinierendes Moment, wenn *„praktisch diese Technik, die man schon, die man schon in Filmen gesehen hat, im realen Leben eingesetzt wird.“* (Aznar de Silva, Vid) Zum Zusammenhang von Technik und Phantasie konstatiert etwa Theo Elm (1991: 61), dass er „die paradoxe Mischung [bildet], die in die Zukunft führt“, denn Fiktion ist nicht nur Spiegel des technisch Möglichen, sondern „faszinierendes Vorzeichen des Hypothetischen“ (ebd.). Wenn das Wissen über die Technologie, das sich in den Interviews abbildet, also auch als ‚mediatisiert‘ (Grusin 2004) zu charakterisieren ist – weil mögliche Zukünfte so bereits vorweggenommen werden –, spielen, wie dann auch Benjamin Muller (2008) konstatiert, Objekte der Populärkultur eine konstitutive Rolle für Bedeutungen und die neuerliche Relevanz der Biometrie. An ihnen, so Muller, lässt sich ablesen, wie Risikotechnologien rationalisiert, fetischisiert werden. Sie (re)produzieren: „claims of efficacy, legitimacy and the general ubiquity of risk management techniques” (ebd.: 214) und konstituieren so auch Bedingungen ihrer Akzeptanz.

Bestimmen lässt sich diese dann nicht nur entlang der „eigenen Annahmen über das aktuell Bestehende, zuvor Gewesene und künftig Erwartbare, sondern auch [...] von anderen gemachten Annahmen“ (Lucke 1998: 16). So kann man, wie Elena Esposito (2007: 120) betont, „die Realität nicht verstehen, wenn man Formen und Bedeutung der Fiktion nicht kennt. Fiktion ist aber etwas anderes als reine Phantasie, weil sie eine eigene Realität entwirft und die fiktive Realität reale Auswirkungen hat“ – sie ist „eine Form der Realitätsverdopplung“ (ebd.: 30f.). Das gilt in gleichem Maße sowohl für die Vorstellungen von den Zwecken, als auch den Risiken, mithin den Sichtbarkeitsregimen, die die Befragten im Hinblick auf die Fingerabdrucktechnologie thematisieren. Ambivalenzen sind demnach auch nicht einfach entlang der Unter-

diesem Zusammenhang eine kritische Aufmerksamkeit erfahren. So wurde dem damaligen Innenminister Otto Schily 2005 für die Einführung des biometrischen Reisepasses der „Big-Brother-Lifetime-Award“ verliehen.

scheidung von objektiv (wahr) oder subjektiv (falsch) zu bewerten, sondern sie entwerfen eine eigene Rationalitätssphäre des Für-Wahr-haltens.

3.2 Vom Subjekt her besehen: Motivlagen und Ambivalenzen

„Welche Maße von Wissen und Nichtwissen sich mischen müssen, um die einzelne auf Vertrauen gebaute praktische Entscheidung zu ermöglichen, das unterscheidet die Zeitalter, die Interessengebiete, die Individuen."
(Simmel 1992: 394)

Die Objektifizierung einer Technologie – sowohl die Aneignung der gegenständlichen Technik als auch des Verfahrens durch ihre Nutzer – ist in erster Linie eine Frage ihrer Platzierung. Sie erfolgt nicht nur räumlich zu bereits vorhandenen Objekten, sondern auch symbolisch in ihrem Verhältnis zu sozialen Beziehungen oder Formen des Gebrauchs. Wendet man eben diesen Zusammenhang, der vor allem in der ethnologischen Forschung zur Aneignung von Artefakten unter dem Begriff der „Domestication" thematisiert wird (vgl. Hahn 2004), dann bedeutet dies, dass Akzeptanzhandeln insofern als situativ zu begreifen ist, weil etwa Ziele und Handlungsabsichten (die Technologie zu nutzen) erst angesichts spezifischer sozio-technischer Zusammenhänge und auch erst in der Situation entstehen können. Dem Nutzungshandeln müssen folglich nicht bereits auf die Technologie gerichtete Absichten zugrunde liegen, sondern diese können sich zudem auch erst vor dem Hintergrund von in die Handlungspraxis eingelassenen Vorannahmen und Deutungsrepertoires entfalten oder entlang einer symbolischen Bedeutung des Verfahrens hervorgebracht werden. Eingang in die Sinnsetzungsprozesse der Befragten finden also sowohl routinemäßige Bedeutungen, aber auch normative Kriterien, die vor allem über die symbolische Bedeutung des Verfahrens hergestellt werden. Das individuelle Akzeptieren zeigt sich dann als variabel: je nach den Handlungsbedingungen, -motiven und -zielen und wird überdies beeinflusst durch die Handlungserfahrungen aufgrund bereits ausgeführter Handlungen, deren Ergebnissen, Folgen und abgeschätzten Wirkungen (vgl. Lucke 1998).

3.2.1 Nutzungsbedingungen zwischen Zwang und Freiwilligkeit

Die untersuchten Anwendungssettings unterscheiden sich im Grad der freiwilligen Partizipation bei der Preisgabe biometrischer Merkmale. Dies gilt auch unabhängig faktischer Nutzungszwänge, wie sie etwa im schulischen Kontext durch bürokratische Erfordernisse oder im behördlichen Setting mit der Fingerabdruckgabe für den Erhalt eines Reisepasses vorausge-

setzt sind. Denn ebenso, wie die sich an die Technologie knüpfenden Zwecke keine „außersozialen Voraussetzungen“ (Hillebrandt 2015: 16) haben, zeigt sich, dass die Wahrnehmung einer Freiwilligkeit oder eines Zwangs zur Datenpreisgabe und mitunter Motive zur Nutzung erst im sozialen, mithin eigensinnigen Ort *entstehen*, in dem ‚Objektives‘ immer erst subjektiv angeeignet wird. Bestimmungen von Freiwilligkeit und Zwang sind in diesem Zusammenhang, erstens, abhängig von expliziten Zwecken, die sich innerhalb eines Settings an das Verfahren knüpfen und, zweitens, von der faktischen Abhängigkeit von dem jeweiligen technischen System in einem Anwendungssetting sowie den hier bereit gestellten Handlungsoptionen sowie, drittens, von situativen Wahrnehmungen während der Registrierungssituation, die in Form wahrgenommener Zwänge Entscheidungen zur Nutzung oder Ablehnung mitunter erst motivieren.

3.2.1.1 Kontroll- und Sicherheitsmotivationen

Kontroll- und Sicherheitsmotivationen stellen das charakteristische Motiv der Nutzung des Verfahrens in den Settings Einwohnermeldebehörde und Schule dar. Eine hier zu beobachtende explizite Vorsorgeorientierung bestimmt nicht nur Wahrnehmungen von Zwang und Freiwilligkeit, sondern sich mit dem Verfahren verbindende Zwecke können objektiv gegebene Zwänge, z.B. im Einwohnermeldeamt, überlagern oder im schulischen Setting erst entstehen lassen.

3.2.1.1.1 Sicherheitsvorsorge

Als zentrale Argumente in den Interviews mit Antragstellern von Ausweisdokumenten erweisen sich Überlegungen, sich mit der Aufnahme der Fingerabdrücke in die Personaldokumente gegenüber zukünftigen Unabwägbarkeiten abzusichern. Dabei findet sich vielfach das Motiv, dass man auf Kontrollanforderungen vorbereitet sein und, zum Beispiel mit Blick auf Grenzkontrollen, lieber nichts falsch machen möchte. Herr Janßen etwa greift mit der Integration seiner Fingerabdrücke in den Personalausweis konkret potentiellen Unannehmlichkeiten vor, die sich im Rahmen eines geplanten Besuchs bei seinem, im außereuropäischen Ausland lebenden, Sohn ergeben könnten. Aus diesem Grund möchte er all seine Papiere *„fertig haben, dass ich keine Schwierigkeiten unterwegs habe.“* Diese Argumentationen korrespondieren mit einer generellen Vorsorgeorientierung in der Kriminal- und Sicherheitspolitik. Während der Fingerabdruck in den Ausweispapieren erklärtermaßen der Prävention von Terrorismus die-

nen soll und im Bezug auf die eher abstrakten Einführungsgründe so auch in den Interviews regelmäßig thematisch wird, bereiten sich die Nutzer folglich auch präventiv auf neue Kontrollprozeduren vor, um keine eventuellen Nachteile zu erleiden, denn: *„falls man reisen möchte, ist man vorbereitet"* (Susanne Jeske, Einwo). Dabei klingt mitunter auch durch, dass Reisen und Grenzkontrollen so beeindruckend (und indirekt auch einschüchternd) sind, dass man da lieber nichts falsch machen möchte:

> „Und ich denk', es wird auch jetzt mehr Möglichkeiten geben, wenn der Staat damit anfängt, dass man halt besser identifiziert werden kann, dass auch, wenn ich mal nach Amerika reise, oder was weiß ich, die haben ja auch strenge Maßnahmen, die man einhalten muss, und das is' ja dann schon besser, wenn man gleich so'n guten Ausweis hat, mit Fingerabdrücken, dass die das überprüfen können. Grad wegen diesem ganzen Terror da. Falls man reisen möchte, ist man vorbereitet." (Susanne Jeske, Einwo)

Mitunter wird also das Risiko, im Zusammenhang mit einem USA- oder Australienflug am Flughafen aufgrund erhöhter Sicherheitsmaßnahmen Probleme zu bekommen oder gar abgewiesen zu werden, als so groß eingeschätzt, dass der Fingerabdruck in den Reisedokumenten eine Art Vorsorge für möglich negative Folgen neuer Kontrollen darstellt.

Zeigt sich hier die Relevanz des Sicherheitsdiskurses für die Akzeptanz, der die Einführung und Durchsetzung von Kontroll- und Überwachungstechnologien untermauern kann (vgl. Traut et al. 2010: 15), wird diese zudem durch die, sich in den Interviews vervielfältigen, Ausdeutungen von Sicherheitszwecken unterstrichen. So formen sich die Thematisierungen von Sicherheit, deutlicher noch als die Äußerungen zur Bequemlichkeit, weniger zu einem einheitlichen oder konstanten Konzept. Stattdessen erweist sich Sicherheit als „Behälterbegriff" (Spreen 2010: 192), den ein Konvolut von mitunter „alltagskulturellen Äußerungen von Sicherheit" (Eisch-Angus 2009: 69) umgibt, in denen lebensweltliche und diskursiv vermittelte Unsicherheiten miteinander verwoben werden. Katharina Eisch-Angus, die dem Thema Sicherheit „als totaler Tatsache" etwa in Alltagsgesprächen (2009: 71) nachspürt, begreift das Thematisieren von Sicherheit, analog zu Charles Sanders Peirces Modell der Zeichen, als einen dialogischen Prozess. Und in der Tat lässt sich die Rede von Sicherheit auch in den Interviews dadurch charakterisieren, dass mitunter ein Topos den anderen ergänzt, wie etwa bei Frau Wilde im Einwohnermeldeamt, bei der gleichwohl die situativen Zwänge (vgl. Kapitel 3.2.1.3) veranlassten, die Fingerabdrücke in den Personalausweis nicht aufnehmen zu lassen:

> „also 'ne eigene Sicherheit, wenn etwas passiert. Wenn ich jetzt viel unterwegs bin oder so und es sollte mal was sein, dass man das noch schneller nachvollziehen kann, die Zuordnung, nich'? Oder jetzt, wenn, ja, aber es müssen ja, wie gesagt, wirklich dann die Angst da sein, Zugunglücke, wo wirklich alles durcheinander geht, wo dann nur noch 'n Rest-Ausweis is' mit 'ner kleinen Chipkarte, wo man dann eben gucken

> kann, da haben wir wenigstens noch ‘n Fingerabdruck. Und dass man das zuordnen kann mit Namen, aber sonst? Ich denk mal, das is‘ eher ‘ne Angst irgendwo zu bleiben und dass man nich‘ nachvollziehen kann, wer da nun is‘.“

Die Rede von Sicherheit ist hier eng verknüpft mit Angstdiskursen. Von einer allgemeinen Notwendigkeit der Identifikation entfaltet Frau Wilde das potentiell Mögliche – *„wenn was passiert“* – in angstbesetzten Szenarien eines diffusen *„Verlorengehens“* und mutmaßt dann auch, dass die Akzeptanz der Fingerabdrücke in den Ausweispapieren von eben solchen Ängsten affiziert sein könnte. Ist zwar das dialogische Prozessieren von Bedeutung gewiss auch durch den verwendeten Interviewleitfaden strukturiert, nähern sich die Befragten auch durch selbst aufgeworfene Assoziationen und Bedeutungszusammenhänge einem solchen Sinn der Technologie an. Dass dabei seltene, aber außergewöhnliche Ereignisse offenbar als normal und erwartbar wahrgenommen und gehandhabt werden, zeigt, dass nicht nur das, was die Befragten wissen, ihre mit der Aufnahme der Fingerabdrücke zum Ausdruck gebrachten Sicherheitsambitionen bestimmt, sondern auch was sie sich schlicht nur vorstellen können. Zeigt sich dies am deutlichsten entlang der thematisierten Flugzeug- oder Bahnkatastrophen, dann werden in diesem Zusammenhang auch ganz persönliche Betroffenheiten relevant. So sind es insbesondere gemeinsam interviewte ältere Ehepaare, die jenes Szenario der schweren Unglücke thematisieren. Sie thematisieren eine persönliche, mitunter sogar intime Sicherheitsrelevanz. Zwar hebt die Speicherung der Fingerabdrücke nicht das potentielle Unglück selbst auf, aber mit ihrem Versprechen auf eindeutige Identifizierung, mithin einer Versicherheitlichung von Identität in Katastrophenfällen, entlastet sie zumindest einen der Ehepartner von der Furcht vor dauerhafter Ungewissheit über den Verbleib des anderen.

In der Logik proaktiven Sicherheitshandelns, so Francois Ewald (1998), wird die Prävention zur Vorbeugung. Es gilt angesichts sich vervielfältigender Unsicherheit (vgl. Bonß 1995: 222) möglichst antizipatorisch das mögliche Schadensereignis vorweg zu nehmen und dafür zu sorgen, dass es nicht eintritt. Bietet sich der Fingerabdruck geradezu als Sicherheitsmaßnahme zur Vorbeugung des Katastrophalen an, dann wäre es angesichts der möglichen Szenarien „riskant, darauf zu verzichten“ (Bröckling 2004: 213), und dies unabhängig davon wie unwahrscheinlich der Worst-Case sein mag. So setzt das Szenario doch, so Susanne Krasmann et al. (2014: 23) gerade auf die Fantasie und Risiken und Ungewissheiten sind zu gleichen Teilen real wie unwirklich. Sind sie der Modus wie Zukunft antizipiert wird (vgl. Krasmann 2007: 307, O’Malley 2004: 15), dann entsprechen diese Überlegungen der Befragten auch einer Logik der Sicherheitspolitik, die sich vor allem über das katastrophische Imaginäre bestimmt, in der bereits das lediglich Vorstellbare zum Anlass für präventives Handeln wird:

„precaution“ besteht „zunächst einmal darin, alle möglichen Bedrohungen zu imaginieren – und zwar in der schlimmstmöglichen Form“ – statt um präventive Risikoabwehr geht es um „hyperpräventive Risikoerfindung“, so Bröckling (2012: 101, mit Bezug auf Frankenberg 2010: 119ff.) in seiner Charakterisierung gegenwärtiger sicherheitspolitischer Gefahrenbewertungen.

Die thematisierten Ungewissheiten, d.h. die Bedrohungsantizipationen – seien es Terrorismus, der katastrophale Notfall oder die Möglichkeit der fälschlichen Identifizierung – deuten dann auch auf ein affektives Moment (vgl. Massumi 2010: 54) des Akzeptanzhandelns. Angst ist dabei nicht individuell zu verstehen, sondern als eine gemeinsame Erfahrung von Verunsicherung, wie sie etwa auch mit dem Begriff einer „Kultur der Angst“ (Furedi 2005) angedeutet wird und der sich darauf bezieht, dass Angst zunehmend eingefordert wird und potentielle Risiken sich dann auch real anfühlen. Zum einen scheinen die Narrative wie der Identitätsdiebstahl wie ein „affektiver Umschlagplatz“ (Opitz 2014: 272) von Angstkommunikation zu fungieren, an dem diese und mithin die Nutzungszwecke der Technologie hervorgebracht werden. Ängste erweisen sich dann als handlungsleitend, wenn Fingerabdrücke etwa präventiv in den Ausweisdokumenten genutzt werden, weil Identifikationsprozeduren an Grenzen als einschüchternd und *„unangenehm“* (Torsten Hildesheimer, Einwo) erlebt wurden oder in dieser Form erwartet werden. Mitunter werden auch aufgrund des symbolischen Moments des Fingerabdrucks, als Zeichen für den notwendigen Schutz vor etwas potentiell Bedrohlichem, Ängste vor Ungewissheiten hervorgebracht, die etwa der Ehepartner bei einem schweren Unglück und der Unmöglichkeit von Identifizierungen ausstehen könnte. Das Angebot zur Fingerabdruckabgabe vermag dann auch selbst zu affizieren, weil Ängste oder diffuses Unbehagen thematisch werden, die sich mit entscheidungsbestimmenden Haltungen verbinden können – etwa als explizite Absicherung gegenüber „Identifizierungs-Notfällen“ oder in Form einer ausdrücklichen Ablehnung, weil der Fingerabdruck als Spur die fälschliche Beschuldigung riskiert – wie unwahrscheinlich dies auch immer scheinen mag, wie folgender Befragter erklärt:

> „ja wenn ich irgendwo jetzt an ‘ner staatlichen Stelle da in USA meinen Fingerabdruck abgebe, das kann ja sein in ‘ner sonstwas Datenbanken landet und ich reise da rum und fasse irgendwo ein Glas an, wo irgendwie ein potentieller Al-Qaida-Mensch da auch irgendwie nebenher ein‘ Kaffee getrunken hat und schon kann ich ganz andere Probleme kriegen.“ (Carsten Welzer, Einwo)

Das Unbehagen angesichts einer fälschlichen Verdächtigung, weil sich der Fingerabdruck jederzeit ‚selbstständig machen‘ kann, existiert auch unabhängig von konkreten Erfahrungen bzw. wirkt letztere nicht zwangsläufig auf die Akzeptanz zurück: Während Herr Lambrecht

etwa die Aufnahme der Fingerabdrücke aufgrund einer bereits erlebten falschen Beschuldigung durch die Polizei ablehnt, steht für die 21-jährige Frau Jeske staatliche Überwachung, die sie, wie sie berichtet, ebenfalls bereits am eigenen Leib aufgrund eines fälschlichen Verdachts erfahren hat, geradezu im Zeichen der Notwendigkeit, Sicherheit herzustellen, wie sie erläutert:

> „Ich hab‘n persönlichen Fall, dass mal die Wohnung von meinem Bruder aufgrund von Verdächtigungen auseinander genommen worden is‘, von der Polizei und die Verdächtigung war eigentlich unbegründet, und unsere Daten sind auch alle mit da rein geflossen, obwohl wir damit gar nichts zu tun haben. Und mein Handy wurde abgehört […]. Das ging ja dann schon wieder um Sicherheit. Man musste ja Verdächtige überprüft werden und so weiter, den Vorgang kann ich auch verstehen, aber ich find‘s halt nich‘ so witzig, dass ich persönlich mit hineingezogen worden bin, obwohl ich damit gar nichts zu tun hatte. Nur weil ich zur Familie gehöre, aber das is‘ ja auch so, dass alle Freunde überprüft worden sind, der ganze Kreis der Bekannten und Verwandten wurde ja überprüft und das darf man nich‘ persönlich gegen sich sehen in solchen Angelegenheiten. Das musst ich aber auch lernen bei meinem Job.“

Der Fingerabdruck, als traditionelle Sicherheitstechnik, sei daher aus ihrer Sicht im Ausweis geeignet, die Möglichkeiten der Strafverfolgung zu verbessern und eine gegebenenfalls notwendige Maßnahme auf dem Weg dorthin. Die von den Befragten zum Ausdruck gebrachten Vorsorgeorientierungen beziehen sich folglich auch auf die Wahrnehmung von sich vervielfältige (Un-)Sicherheitslagen, wie sie auch in den zahlreichen Ausdeutungen der Versicherheitlichung von Identität ihren Ausdruck findet. Cole und Pontell (2006: 196) erkennen hierin dann auch ein Merkmal der „soft surveillance“ als Bestandteil eines allgemeinen Responsibilisierungsdiskurses, denn wenn es das Ziel ist, alle denkbaren Formen des Gefahreneintritts zu antizipieren, dann ist Vorsorge zentral (vgl. Ewald 1998):

> „we argue that the contemporary ‚panic‘ discourse surrounding identity theft is an example of ‚soft surveillance‘, in which individuals are encouraged, or even required, to take responsibility for their own protection.“ (Cole und Pontell 2006: 196)

In diesem Zusammenhang wird dann auch der Zwang zum Fingerabdruck im Reisepass, der gesetzlich verankert eigentlich die Wahrnehmung von Optionen ausschließt, von den Befragten auch nicht nur als ein eben solcher gedeutet, etwa als bürokratische Routine, die man *„akzeptieren muss“* (Torsten Hildesheimer, Einwo), sondern auch als eine Frage der Freiwilligkeit verhandelt. Hier findet die doppelte Logik der Sicherheitsproduktion, die Louise Amoore (2008: 23ff.) für den gegenwärtigen Einsatz biometrischer Systeme konstatiert, immer dann seine Entsprechung, wenn die Speicherung der Fingerabdrücke zum Preis wird, den man für die ständige Aufforderung bezahlt, die eigene Identität zu bestätigen. So argumentieren einige Befragte, dass man ja Handlungsoptionen besäße – in den Worten der 45-jährigen Frau Ama-

rell: *„es zwingt mich ja keiner, in die USA zu fliegen oder in außereuropäische Länder."* Das Recht auf Handlungsfreiheit (Art 2 Abs. 1 GG), zu dem die Reisefreiheit gehört, wird so aufgegeben. Oder umgekehrt wird der Reisepass zu einem Produkt, das man ‚erwirbt' oder erwerben kann, um reisen zu können. Das Recht wird gleichsam kommodifiziert, oder wie Benjamin Goold (2010: 14) resümmiert: „Consumers of the consumption decisions of others indirect consumers of security goods exercise autonomy and choice" und in den Worten von Frau Jeske (Einwo): *„kauft"* man *„sich ja 'n Reisepass, um überall hinreisen zu könn', wo man hin möchte."*

3.2.1.1.2 Kontrollmotive

Umdeutungen von Zwang in Freiwilligkeit lassen sich auch im schulischen Kontext identifizieren. Wenngleich die Vorgabe für ein bargeldloses Bezahlvorfahren obligatorisch ist, um von Essenssubventionen zu profitieren, bilden die Ausführungen von Frau Walter (vgl. Kapitel 3.1.1.2), die das Verfahren als bequeme Kontrollmöglichkeit erfährt, das sie von finanziellen Planungen entlastet, ein Beispiel für die spezifische Adaption einer auch zu Zwecken der Kontrolle der Sozialleistungsberechtigung implementierten Technologie. Frau Walter arrangiert sich nicht nur mit einem, ihrer Familie mehr oder weniger, verordneten Verfahren, sondern entwickelt daraus individualisierte Handlungsoptionen für ihre im Verlauf des Interviews als finanziell prekär beschriebene Situation. Eine solch technologisch mediierte und paternalistische Kontrolle des Sozialleistungsbezugs durch die „Verfingerabdruckung von Wohlfahrtsleistungsbeziehern" (Nogala 2000: 73) wird von ihr nicht als Zwang gedeutet. Ebensowenig sieht sich subjektiv Handlungseinschränkungen ausgesetzt oder empfindet Gefühle der Erniedrigung. Vielmehr lässt sich ihre Haltung mit Harry Murray (2000) als eine Ausdrucksform von „deniable degradation" verstehen, denn damit Degradierung effektiv wird, muss sie auch als solche empfunden werden.

Gewiss ist an dieser Stelle ein Intervieweffekt denkbar, weil entsprechende Erfahrungen als derart unangenehm empfunden werden, beziehungsweise mit Scham besetzt sind, dass sie als nicht-thematisierbar gelten. Ebenso naheliegend erscheint es aber auch, dass sich die betroffene Mutter schlicht nicht automatisch „in der Singularität dieses Abdrucks für die Zwecke einer Administration [subjektiviert], die einen von nun als Objekt verwalten kann und wird" (Legnaro 2011: 197). So bedeutet das Verfahren für sie vielmehr, dass Verwaltungsprozesse, die faktisch ihre Legitimierung für den Bezug von Sozialleistungen begleiten, vereinfacht, und sie selbst von eigenen Kontrolltätigkeiten entlastet wird. In diesem Zusammenhang über-

lagern sich dann auch Bequemlichkeitsversprechen und Erwartungen von Sicherheit: Weiß Frau Walter mit dem Fingerabdruck-Onlinebezahlverfahren das zur Verfügung stehende Haushaltsgeld auf bequeme Weise sicher angelegt, dann fungiert es für sie vor allem als ein Für- und Vorsorgesystem in vergleichsweise prekären Sozialverhältnissen. Mit einem solchen Sicherheitsfokus – auf das individuelle materielle Lebensniveau, das es zu gewährleisten gilt und das nur schwerlich finanzielle Einbußen verkraften kann – leitet sie aus der Eindeutigkeit des Fingerabdrucks dann auch, am Beispiel des Einsatzes zur Zeiterfassung, Funktionen des Verfahrens ab, die es, über den schulischen Anwendungsbereich hinaus, für sie vor allem als Instrument qualifizieren, um arbeitsrechtliche Gerechtigkeit herzustellen:

> „Gastronomie vielleicht. Damit die Leute mal sehen, was die Leut‘ schaffe, an Stunde‘. Fabriken, aber die haben‘s ja eh schon, ne, die haben ja die Büros. Alles Büros. Angefangen von Krankenkassen, damit die mal sehen, wie oft sie Kaffee trinke gehen ((I lacht)). Ja.“ (Sabine Walter, Schul2)

In den Schulen bestehen also unterschiedliche Ausgangsituationen für Akzeptanz, die, zum einen, in unterschiedlichen Funktionen der Biometrie begründet sind bzw. nur indirekt mit dem Verfahren selbst verknüpft sind. Das Setting Schule ist, zum anderen, ein besonderer Fall, weil hier neben Schülern auch die Eltern in den Prozess des Akzeptierens involviert sind, und damit ein weiterer Akteur, der weder Abdrucknehmer noch selber zu registrierender Abdruckgeber ist und dessen Entscheidungen zur Nutzung des Verfahrens, wie gezeigt, vielfach von expliziten Kontrollintentionen geleitet sind. Dies lässt die nachfolgend zitierte Passage aus einem Interview mit einer Mutter noch einmal deutlich werden:

> „Das war ja damals ganz am Anfang, als wir die Mensa hier bekamen, da wurde das dann gleich vorgestellt und ich hab‘ mir eben überlegt, es wurden natürlich die ganzen Vorteile da angepriesen, einmal, dass die Kinder kein Geld dabei haben müssen und dass sie‘s nich‘ verlieren können. Das war also auch ‘n Aspekt, der bei uns dann ((lacht)) auch wichtig war, aber eben auch diese Erpressung. Es wird ja immer schlimmer an deutschen Schulen, weiß jetz‘ nich‘, ob das hier so is‘ ((lacht)) (I: Oh, ja?) Ja. Ich mein, jetz‘, hier is‘ mir das nich‘ bekannt, aber an anderen Schulen, wo gesagt wird: Hier komm, Geld her oder wir, oder wir schlagen dich zusammen oder sowas, ja also. Um das Kind von daher auf jeden Fall unangreifbar zu machen.“ (Monika Reckling, Schul1)

In der zitierten Passage fällt der ebenso pessimistische wie spezifisch kriminalitätsorientierte Betrachtungswinkel auf die Vorteile des Verfahrens auf: Aus einem pädagogischen wird ein gefahrengeneigter, mithin gefährlicher Ort und dies auch unabhängig faktischer Relevanz. Deutet sich hier an, dass kriminalitätsassoziierte Risiken der Bargeldmitnahme im Rahmen der Einführung des Verfahren thematisch wurden, wird mit dieser diskursiven Rahmung zudem ein Risiko durch delinquente Mitschüler kreiert, das sich theoretisch auch an dieser

Schule realisieren könnte. Schule wird danach zu einem Setting, das besondere Schutzmaßnahmen notwendig macht und das Verfahren gleichsam von sich aus legitimiert, weil es das Kind sowohl vor physischer Gewalt als auch Nötigung bewahrt. Wird das Direktmarketing von Überwachung ermöglichenden Technologien an Schulen regelmäßig als materielle und symbolische Manifestation einer Kultur der Kontrolle (vgl. z.B. Monahan 2006: 117) und als Indiz für eine neue, etwa von Cindy Katz (2006) als „hypervigilance" bezeichnete elterliche Übersorge diskutiert, ergeben sich mit Kontrollambitionen verknüpfte Nutzungsmotive, wie bereits dargestellt, mitunter aber teils nur vermittelt über das Verfahren selbst. Denn erst mit dem online verfügbar gemachten Abrechnungssystem erweitert sich die Möglichkeit, weitere Vulnerabilitäten zu konstruieren. Die Kinder *„unangreifbar"* (Monika Reckling, Schul1) zu machen, erweitert sich dann vom Schutz vor Kriminalität auf jene Ernährungsrisiken, die von den Kindern selbst ausgehen und insofern auf selbst verschuldete Verletzlichkeiten.

Vor diesem Hintergrund lassen sich Akzeptanzbedingungen für die Schüler daher auf unterschiedlichen Ebenen ausmachen, die teils quer zum Verhältnis von Freiwilligkeit und Zwang liegen. So überlagern sich, erstens, settingspezifische Vorgaben, *„weil man da Vergünstigungen bekommt"* (Malte Günthner, Schul1) und elterliche Entscheidungen. Retrospektiv berichten Schüler etwa: *„ich hab's halt gemacht, weil's meine Eltern gesagt haben"* (Miriam Soeffner, Schul1). Den Hintergrund hierfür bilden dann auch mitunter die expliziten Kontrollintentionen, wie sie sich etwa bei Herrn Flieger zeigen. Auf die Frage, ob die Entscheidung zur Nutzung des Verfahren vorab mit dem Sohn diskutiert wurde, erklärt er:

> „Mmm, nein ich hab' ihm, bevor ich's gemacht hab, schon gesagt: ‚So werden wir das in Zukunft handhaben'. Aber, ich war jetzt nicht so derjenige, der gesagt hat: ‚Willst du das so und bist du damit einverstanden.' Das sicherlich nich', weil ich ganz klar die Antwort kriegt hätt': ‚Nee. Mir is' das lieber, wenn ich mein Geld mitnehme'. Und wenn ich, am besten jeden Tag bei Mama nach Geld frag' und das dann auch jeden Tag ordentlich ausgeb'." (Wolfgang Flieger, Schul1)

Mit den von Herrn Flieger antizipierten Widerständen seines Sohnes lässt sich diese Nutzung als ein ausdrücklicher, fernab bürokratischer Notwendigkeiten von elterlichen Sicherheitsorientierungen geleiteter, Zwang ausweisen. Gleichwohl nehmen die Eltern diese Kontrollmöglichkeiten mitunter auch erst nach und nach wahr und Nutzungsintentionen gehen, zweitens, auch von den Schülern aus, die etwa ihrer Begeisterung an der neuen Technik nachgehen dürfen. Diese entfaltet vor allem für die jüngeren Schüler den Reiz des Neuen, und – ausschließlich in diesem Setting – auch ein spielerisches Element, wie es z.B. Ellerbrok (2011: 538) als „the lighthearted use of a technology or technological system for purposes of personal entertainment, amusement, or fun" beschreibt. Auch die 12-jährige Vanessa Klein (Schul2), die

zwar zur Nutzung eines bargeldlosen Bezahlsystems verpflichtet ist, damit sie Essenssubventionen in Anspruch nehmen kann, findet es etwa *„immer so cool wenn‘s leuchtet und dann da drauf legen. Ja ich find‘s cool.“* Für viele andere Schüler hingegen weicht die Erfahrung dieses Neuartigen oder Spannenden im zeitlichen Verlauf einer Wahrnehmung der Technologie als einer Bezahlmethode, die im Vergleich mit anderen verfügbaren Alternativen zwar Vorteile aufweist, weil sie bekannte Abläufe beschleunigt, wenn etwa die Kassiererin nur noch *„auf‘n Knopf [zu drücken braucht] und weil sonst müsse se alles eingeben.“* (Luca Michaelis, Schul2). Letztlich erscheint das Verfahren im praktischen Umgang für die Schüler dann aber vor allem auf diese Funktion zentral, wie etwa der 12-jährige Giovanni Pirlo (Schul2) erklärt:

> I: „Und in der Zeit als es funktioniert hat, war für dich mit dem Finger zu bezahlen genauso wie wenn du mal was bar zahlst und mit Geld?“
>
> Giovanni: „Es ging eigentlich, ich fand‘s halt praktischer, aber so is‘ eigentlich dasselbe.“

Drittens können sich bürokratische Bestimmungen sowohl mit praktischen, das heißt bequemen, Anwendungszwecken und elterlichen Sicherheitsorientierungen überlagern. Mit der Nutzung des Verfahrens wähnen sich die Schüler *„auf der sicheren Seite“* (Giovanni Pirlo, Schul2), da sie sich gegenüber den Eltern von dem Risiko des Bargeldverlustes entlastet fühlen, wie auch die Sequenz aus dem Interview mit dem 9-jährigen Luca Michaelis (Schul2) verdeutlicht:

> I: „Habt ihr denn da vorher mal näher darüber geredet, dass du das machen willst, mit deinen Eltern oder in der Klasse?“
>
> Luca: „Mit meinen Eltern. Weil das is‘ ja besser, weil wenn du Geld mitnimmst, kann man‘s ja verlieren.“
>
> […]
>
> I: „Ja, ok. Macht dir das auch Spaß das zu benutzen?“
>
> Luca: „Ja, weil dann hat man nicht die Angst, dass man das Geld verlieren kann.“

Auffällig erscheint hier, dass die Antwort auf die Frage nach dem „Spaß“ im Umgang mit der Technologie, die sich ursprünglich auf die von Luca wahrgenommenen Vorteile bezog, von ihm als konkrete Reduktion von Unsicherheitsmomenten formuliert wird. Den Zusammenhang zwischen der Technologieverwendung, elterlichen Ängsten und ihre Reflektion in kindlichen Wahrnehmungen zu eruieren, wie er sich hier lediglich andeutet, muss allerdings Aufgabe weiterer Forschung bleiben.

3.2.1.2 Ambivalenzen der Automatisierung

Mit der durch das Verfahren ermöglichten Automatisierung stellt sich für Nutzer die Frage nach Zwang und Freiwilligkeit dann auch auf der Ebene der konkreten Benutzung. Die settingspezifische Integration, zu der auch die Einbindung des Verfahrens in größere technische Strukturen gehört, variiert im Hinblick auf verfügbare Handlungsalternativen und führt zudem zu spezifischen Abhängigkeiten, etwa vom Funktionieren der Technik, und bedingt spezifische Anschlusshandlungen, die die sich mit der Technologie verbindende Zweckmäßigkeit mitunter relativieren.

3.2.1.2.1 Nebeneffekte des Verfahrens

In den Schulen erweist sich eine gegebenenfalls von den Eltern vorgenommene Kontrolle, die durch das automatisierte Abrechnungssystem ermöglicht wird, zumindest für die befragten Schüler als nachrangig. Von Relevanz ist für sie hingegen das konkrete Funktionieren des Verfahrens. Die Ambivalenz der Automatisierung, die sich aus einem Nicht-Funktionieren ergeben kann, konkretisiert sich in einem, in beiden Schulsettings implementierten, System informellen Kreditgebens: Weil sich Fälle häuften, dass Mittagspreise nicht per Fingerabdruckverfahren im Kassensystem verbucht werden konnten, führen die Kassiererinnen parallel eine handschriftliche Liste, in der namentlich jene Schüler eingetragen werden, denen trotz Nichtfunktionierens des Bezahlverfahrens Essen ausgegeben werden. Liegt der Vorteil darin, dass die betroffenen Schüler nicht hungrig bleiben – ein Aspekt, der die Relevanz des Verfahrens infrage stellen würde –, ist dies für die Schüler mitunter nicht unproblematisch. Die eigentlich von dem Verfahren begeisterte Vanessa Klein (Schul2), die, weil es ihren Fingerabdruck *„irgendwie nicht mehr gibt“*, ihre Käufe seit etwa einem Monat aufschreiben lassen muss, *„nervt“* das sehr, wie sie erklärt:

> I: „Ok. Und wie findest du das, dass das jetzt irgendwie nicht geht?“
>
> Vanessa ((stöhnt)): „Hmmm, gut ich find‘s nich‘ gut, also ((Geräusch mit den Lippen)) hmhm ((ablehnend)) nicht gut.“ ((kurzes Lachen))
>
> I: „Warum nich‘?“
>
> Vanessa: „Jaa, das nervt mich. Weil immer wenn ich da stehe, muss ich des dann aufschreibe aufe Zettel. Also geht nicht mit dem Finger, ich muss mein‘ Name aufschreibe, was ich gekauft hab. […] Ja, es dauert ein bisschen lange an der Kasse und dann, die anderen Kinder warten dann immer so lange und das dauert ja mindestens 30 Sekunden, musst das aufgelegt werden und dann geht wieder nicht.“

Das Aufschreibsystem führt ein neues Element in das Setting Bezahlen in der Schulmensa ein, wodurch es dieses verändert. Es verlängert nicht nur den einzelnen Bezahlvorgang – wenn zunächst erst mehrmals der Fingerabdruck auf den Scanner gelegt wird und dann die Eintragung der so entstandenen *„Schulden"* (Theresa Valentin, Schul1) sowie Name, Jahrgangstufe und Geburtsdatum in die Liste vorgenommen werden muss und andere Schüler deshalb länger warten müssen. Die Substitution des Nicht-Funktionierens durch das Aufschreibsystem erzeugt zudem eine Aufmerksamkeit, die das ursprüngliche politische Argument, wonach mit der Verpflichtung zum bargeldlosen Zahlungsverkehr Sozialleistungsansprüche und damit soziale Unterschiede gerade in der Technologie verschwinden sollen, konterkariert. Denn Vanessa, weil sie regelmäßig den Sonderfall des Aufschreibens in Anspruch nehmen muss, ist damit exponiert. Alternativen des Bezahlens sind für sie nicht zur Hand, denn die Mitnahme von Bargeld als ‚Notausgang', falls das Verfahren nicht funktioniert und wie es andere Schüler nutzen können, ist für Kinder, deren Eltern Vergünstigungen für das Mittagsessen in Anspruch nehmen wollen, keine Alternative, da mit der Barzahlung der volle, statt der reduzierte Preis zu zahlen wäre.

Die spezifische Bedeutung des neuen Elements – Bloßstellung zu verursachen – lässt sich vor allem in Interviews mit anderen Schülern eruieren,[56] denn obzwar es für die befragten Kinder und Jugendlichen, ihren Aussagen nach, keine Rolle spielt, ob Mitschüler Essensvergünstigungen erhalten oder nicht, zeigt sich hingegen etwa im Gespräch mit der 12-jährigen Maria Reckling und ihrer gleichalten Freundin Steffi Drobnic, die beide das untersuchte Gymnasium besuchen, dass es durchaus als Makel erachtet wird, namentlich auf der ‚Anschreibliste' geführt zu werden:

> Maria: „[…] dann steh'n immer ganz große Listen da und dann der und der zum, zur Kasse kommt und dann finde ich's vielleicht bisschen peinlich, wenn dann da oben mein Name stehen würd'."
>
> I: „Passiert das manchmal, so Mitschülern von dir?"
>
> Maria: „Also ja (I: Die das machen müssen), es sind schon mal zwei von meiner Klasse drauf und von deiner Klasse standen (Steffi: Ja) auch schon mal welche dran."
>
> I: „Und das is' dann ein bisschen peinlich?"
>
> Maria: „Eh ja ((stöhnend))."
>
> Steffi: „Meistens sind's die Jungs."
>
> I: „Ehrlich?"
>
> Maria: „Also bei uns war'ns zwei Mädchen."

[56] Vanessa wurde hierzu bewusst nicht weiter befragt, um nicht einen potentiellen Stigmatisierungseffekt zu produzieren und sie selbst thematisierte diesen Effekt nicht.

> Steffi: „Bei uns war‘ns die Jungs?“
>
> I: „Sag, passiert denen das öfter, oder?“
>
> Steffi: „Ich glaub, dem ist‘s zweimal passiert und hat’s Geld vergessen. Und er wusst‘ das dann nich‘ und dann stand er da.“

Die Schülerinnen empfinden die Vorstellung, Teil einer solch öffentlich ausgestellten Liste zu sein und damit sichtbar zu werden, zwar nicht als degradierend, da in diesem Interviewauszug keine spezifisch neuen Identitätszuschreibungen zu entdecken sind, hinter denen alte Charakteristika verschwinden. Dennoch wissen die Mädchen sehr wohl genau, wer bereits ‚Teil der Liste‘ gewesen ist und verweisen mit dem Begriff des „Peinlichen“ auf eine Furcht vor einem solchen „Stigma“ (Goffman 2010), ohne dass sich jedoch im Interview weiter eruieren ließe, was den konkreten Entwurf darstellt, von dem sie fürchten, abweichen zu können.

Auf den von den Kassiererinnen der Mensen geführten handschriftlichen Listen werden auch „Schulden“ registriert, die durch nicht hinreichende Deckung des in das Bezahlsystem integrierten Treuhandkontos entstehen. Auf der Nutzungsebene geht damit teilweise eine Entstrukturierung des Handelns einher, da die Handhabung des mit dem Fingerabdruckverfahren verbundenen Onlinezahlverkehrs für einige Schüler mit einem erhöhten Handlungsaufwand verbunden ist, der die mit der Technologie assoziierte Bequemlichkeit relativiert. Denn von dieser zu profitieren, bedeutet, das gesamte, das Verfahren umgebende, Bezahlsystem zu beherrschen, wie der nachfolgend zitierte 17-jährige Malte (Schul1) in Bezug auf seine Erfahrung als mehrjähriger Nutzer ausführt:

> Malte: „Ja, am Anfang war‘s auch so, da wurde zum Beispiel der Fingerabdruck nicht erkannt oder bis das Konto erst richtig lief und alles, aber, wenn man bis dann das richtig hat, kommt auch Routine rein. Das geht dann eigentlich auch.“
>
> I: „Ja, wieso so Routine bei dir?“
>
> Malt: ((fällt ins Wort)): „Ja, zum Beispiel beim Geld überweisen oder zu schauen halt wie viel Geld hab‘ ich noch, wann muss ich wieder was drauf zahlen, all die Sachen halt oder die Preise auch, bis man dann da so‘n Überblick hat und alles.“

Mit der Einbettung des Fingerabdruckverfahrens in das Onlinebezahlsystem fühlt sich Malte zwar, wie die Mehrheit der Schüler, auf der einen Seite, praktisch und kognitiv von Bargeld entlastet – weil *„man halt nicht ans Geld denken [muss]“*, und, wie er an einer anderen Stelle im Interview erklärt, man *„einfach so einkaufen“* kann. Dafür muss er, auf der anderen Seite, selbst indirekte, das heißt durch das Fingerabdruckverfahren als bargeldloses Bezahlverfahren vermittelte, Kontrollaufgaben übernehmen. Hier entsteht ein technisch induzierter Kontrollzwang, der, aufbauend auf der Funktionalität des bargeldlosen Bezahlsystems, im Gegensatz zu dem Versprechen von Flexibilität und Entlastung des Verfahrens steht. Denn den *„Über-*

blick [zu] behalten" bedeutet für die Schüler ein kontinuierliches Monitoring – vom eigenen Kaufverhalten, über den aktuellen Kontostand bis hin zu Preisveränderungen in der Mensa –, das den Eltern regelmäßig für eine entsprechende Anpassung der Einzahlungen auf das Treuhandkonto zurückgemeldet werden muss. Während Malte sich mit diesem erhöhten Aufwand arrangiert hat, stellt dieser demgegenüber für die 10-jährige Pinar (Schul2) einen gewichtigen Grund dafür dar, das Bezahlverfahren ausdrücklich nicht länger nutzen zu wollen, wie sie erklärt:

> Pinar: „Also am Anfang hab' ich dann immer mit dem Finger bezahlt, manchmal hab' ich auch von zu Hause und wenn ich kein Geld mehr auf'm Fingerprint hatte, hab' ich's meiner Mama gesagt und wir haben's immer vergessen neu zu machen. Also dann ist das so weitergekommen und dann hab' ich letztes Mal wieder drauf gemacht und das ist wieder leer, also muss ich jetzt noch mal."
>
> I: „Hmm, ok. Weil man da immer das Konto auffüllen muss. Deswegen möchtest du das nicht mehr machen, weil dir das so umständlich ist, oder?"
>
> Pinar: „Nein ((nachdrücklich)). Eigentlich will ich halt nur mit Bargeld bezahlen."
>
> Interviewer: „Ok. Warum?"
>
> Pinar ((lacht)): „Ja das ist, weiß ich auch nicht, man vergisst manchmal das Geld aufzuladen und danach dauert's immer so länger und so deswegen mein ich's ja."

Pinar beschreibt im Verlauf des Interviews dann auch den unangenehmen Effekt, der sich aus dieser Form des Nicht-Funktionierens des Verfahrens ergibt, denn der Bezahlvorgang dauert dann nicht nur länger, sondern manchmal *„meckern"* auch die anderen Schüler und dann *„werd' ich schlecht"*. Die Schülerin erlebt das Nicht-Funktionieren als Belastung, das heißt als eine Beeinträchtigung ihrer individuellen Befindlichkeit und Stimmung. Auch die direkt an die Interviewerin gerichtete Frage, ob sie bei einem geplanten Schulwechsel weiterhin zur Nutzung des Verfahren verpflichtet wäre, deutet auf einen subjektiven Leidensdruck.

Dieser und die daraus resultierende explizite Ablehnung ergibt sich aus dem Zusammenspiel eines Zwangs zur Nutzung des Fingerabdruckverfahrens sowie der Erfahrung eines ungewollt ausufernden Nutzungsaufwands, der aus der Einbettung in das größere System des bargeldlosen Bezahlverfahrens und den mitunter peinlichen Momenten resultiert, die sich aus dem Nicht-Funktionieren des gesamten Systems ergeben.

3.2.1.2.2 Abhängigkeit von Technik

Eine doppelte Ambivalenz der Automatisierung durch die Abhängigkeit vom Funktionieren und aufgrund fehlender Handlungsalternativen wird auch von Befragten in der Videothek problematisiert, weil hier die aus der konkreten Anwendung der bequemen Technologie resul-

tierende Handlungserleichterung und Flexibilität, trotz erwarteter Vorteile, ebenfalls keine absolute ist. Sie artikulieren – trotz der Selbstverständlichkeit mit der sich für sie der Umgang mit der Technologie im Rahmen des automatisierten DVD-Ausleihverfahren ergibt – gleichwohl Grenzen der Automatisierung und mitunter auch ein Unbehagen angesichts zunehmender Automatisierung insgesamt, weil der Mitarbeiter vor Ort *„generell schöner“* sei (Florian Grippe, Vid) und *„die persönliche Schiene“* (ebd.) und damit der *„persönliche Kontakt“* (Corinna Meier, Vid) verloren gehen. Diese Wertschätzung des menschlichen Faktors lässt sich darauf zurückführen, dass bekanntermaßen in anderen Videotheken Personal regelmäßig vorzufinden ist, das dann auch bei technischen Problemen zu Rate gezogen werden kann. In der Automatenvideothek kann Hilfestellung demgegenüber nur selten unmittelbar durch den Betreiber erfolgen, was von den Nutzern als Problem wahrgenommen wird:

> „Hat diese Technik irgendein Problem, bin ich aufgeschmissen, komm‘ ich an gar nichts mehr ran (I: Ja), das is‘ eben das. Wenn der Mitarbeiter X in ‘ner Videothek Y krank is‘, denn kommt der Mitarbeiter Z auf‘s Spiel und ich krieg meinen Film trotzdem. Ne? Is‘ der Automat krank, komm ich an nichts mehr ran. Das is‘ vielleicht der Nachteil.“ (Rainer Tapfer, Vid)

Das Risiko der „Erkrankung“ des Automaten können die Nutzer in der Videothek zwar durch eine DVD-Vorbestellung über ein Onlineverfahren umgehen. Während diese Alternative zwar als praktikabel wahrgenommen wird – lassen sich doch auf diese Weise DVDs ausleihen, selbst wenn die Authentifizierung am Automaten nicht funktionieren sollte – schränkt dieser ‚Notausgang‘ aber die eigentlich mit der Automatenvideothek verbundene Flexibilität – per Fingerabdruckverfahren spontan rund um Uhr DVDs ausleihen zu können – ein, wie die 28-jährige Corinna Meier im Gespräch mit dem Interviewer erklärt:

> Corinna Meier ((fällt ins Wort)): „Ja, ‘ne Freundin von mir hatte da schon mal, also ich hab‘ vorher in ‘ner WG gewohnt und die, meine WG-Partnerin, hatte halt den Ausweis vorher, und den haben wir uns halt auch geteilt, weil wenn man online reserviert, braucht man den Fingerabdruck ja auch gar nich‘, dann kann man das sozusagen online reservieren und einfach nur mit der Karte abholen.“
>
> I: „Das heißt in der anderen Videothek aber, oder (Corinna gleichzeitig: Nee, auch in der) auch in der. (Corinna: ja) Dann habt ihr die euch geteilt.“
>
> Corinna Meier: „Genau. Und deswegen war das kein Problem. Also, ist in der Partnerschaft ist das auch so, wenn man, wenn der eine mal nich‘ kann (I: Ja), dann kann der Andere den halt abholen, nur den Finger kann man halt, wie gesagt ((lacht)), nicht mitnehmen. Dann muss man das halt online reservieren und sich zuhause schon überlegen, was man gucken will, was ja aber an sich auch kein Problem is‘, also. Wenn man das mit dem Fingerabdruck völlig umgehen will, würde das glaub ich auch geh‘n.“

So macht Corinna hier auf ein, auch von anderen Nutzern thematisiertes, praktisches Dilemma aufmerksam, dass sich in der Automatenvideothek als eine zweifache Einschränkung der

Flexibilität durch die eigentlich bequeme Technologie erweist: Umgeht man mit der Onlinereservierung das Fingerabdruckverfahren, ist es nicht möglich, spontan einen Film auszuleihen und etwa erst vor Ort eine konkrete Leihentscheidung zu treffen. Die Abhängigkeit vom Funktionieren des Automaten und mithin dem Fingerabdruckverfahren erscheint folglich nicht nur als riskant, sondern unterläuft offenbar auch die Selbstverständlichkeit der gesamten Praxis des Film-Ausleihens,[57] weil das Verfahren, mit Latour (1996) gesprochen, zum objektbezogenen Alleingang verpflichtet. Wenn aus Sicht mancher Nutzer der Videothek Zugangsmechanismen wie ein Kundenpasswort als die *„elegantere"* Lösung (Karsten Gald, Vid) angesehen werden, dann auch deshalb, weil das Fingerabdruckverfahren mitunter ihren Vorstellungen von der medialen Praxis eines Videothekenbesuches selbst zuwiderläuft, kann doch, umgekehrt, mit dem Fingerabdruck immer nur der für das Verfahren registrierte Nutzer von der mit ihm verbundenen Flexibilität profitieren, da man, anders als eine Kundenkarte *„logischerweise den Finger nicht mitnehmen kann"* (Karsten Gald, Vid). Demgegenüber bedeutet umfassende Flexibilität und Bequemlichkeit für die Nutzer aber, dass auch einzelne Handlungsschritte, wie den Film auswählen und/oder diesen *„besorgen",* auf und mit dem Partner (ver-)teilbar wären und man eben, wie ein anderer Befragter erklärt, etwa *„sagen kann, irgendwie, ich geb' dir mal meine Karte mit und sag dir meine PIN und dann log dich da mal ein und hol mal'n Film"* (Max Schaf, Vid). Die Nutzer fühlen sich mit dem Fingerabdruckverfahren folglich auch in eine neue Praktik des Filmausleihens hineingezwungen.

Wenn also der sozio-technische Rahmen typische Erwartungen umschließt, die sich nicht in erster Linie auf die Technologie selbst richten müssen, dann lässt sich ergänzen, dass der Sinn der Technologie in der Regel nicht nur innerhalb „sozio-technischer Konstellationen" (Rammert 2007a: 92, 1988: 174) erschlossen wird. Der Einsatz des Fingerabdruckverfahrens fordert vielmehr auch existierende Strukturen heraus – in anderen Worten können Vorstellungen von und Erfahrungen mit ‚typischen' Praktiken innerhalb der sie umfassenden soziokulturellen Kontexte selbst den nützlichen Zwecken der Technologie zuwiderzulaufen. Dies spiegelt sich nicht nur darin wider, dass etwa die bequeme Filmleihe durch Automatisierung per Fingerabdruck oder das alternative Onlineverfahren in einen Widerspruch mit den sich an ‚klassische' Videothekenbesuche knüpfende Vorstellungen geraten können. Eine solche Interferenz lässt sich auch für das Verständnis für einen scheinbar argumentativen Widerspruch heranziehen, der sich darin zeigt, dass auch Befragte unabhängig entsprechender Benutzungs-

[57] Der Frage, ob sich durch neue Formen des Filmverleihs, z.B. Automatenvideotheken oder Video-on-demand, die Kultur des Film-Leihens verändert, geht zum Beispiel Tobias Haupts (2014) nach.

und damit Erfahrungen des Nichtfunktionierens[58] der gegenständlichen Technik „Notausgänge“ thematisieren. Wenn etwa Supermarktkunden für den Fall des Nichtfunktionierens darauf hinweisen *„eh immer Geld dabei“* (Petra Müller, Sm) zu haben, lässt sich vor diesem Hintergrund auch annehmen, dass es auch bereits schlichte Gewohnheit sein kann, die den argumentativ herausgestellten Mehrwert des Verfahrens in Frage stellt. Die Beobachtungen, wonach die Nutzung des Verfahrens im Supermarkt im Kontrast zu den vergleichsweise etablierten Bezahlverfahren verschwindend gering ist, deuten darauf hin, dass mitunter bereits die Routine des regelmäßigen Mitführens von Portemonnaies resp. Bargeld und/oder EC-Karten den vergleichsweise ermittelten bequemen Vorteil des Verfahrens zu relativieren scheint.

Es lässt sich daran anschließend weiter folgern, dass sich die biometrische Identifikation in einer technologisch durchdrungenen Welt keinesfalls so nahtlos an Passwörter, PIN-Codes oder andere Werkzeuge anschließt, wie etwa Argumentationen nahelegen, die in der zunehmenden Nutzung ein Bedürfnis erkennen, das Leben zu beschleunigen und abzusichern, es mithin mit Bequemlichkeit und geringerem Risiko auszustatten (so etwa Aas 2006: 150, vgl. Weber 2008). Zwar wird das Fingerabdruckverfahren auch im Supermarkt als Ausdruck einer natürlichen Entwicklung hin zu zunehmender Automatisierung bewertet und der zu Beginn angeführte Verweis der Supermarktkundin Petra Müller auf das als vergleichsweise antik erscheinende Schecksystem (vgl. Kapitel 3.1.1.1) erscheint dafür als emblematisches Beispiel. Doch auch wenn die entlastenden Effekte des Verfahrens als willkommen und im Supermarkt in der Regel ausdrücklich befürwortet werden, da sie menschliche Handlungsfunktionen durch materielle Akte ersetzen, erscheint etwa eine Selbstzahlerkasse als finale Automatisierung im Supermarkt, ob nun mit ohne Biometrie, gleichwohl als eine zu weitreichende Technisierung, gar als *„suspekt“* (Petra Müller, Sm) und insofern als fragwürdig.

Mit den thematisierten Notausgängen lässt sich in der Nutzung des Verfahrens dann auch eine Haltung identifizieren, die als eine Gelassenheit zu den Dingen zu charakterisieren wäre: Gebrauchsdinge zur Erleichterung zu nutzen, ohne gänzlich in der Technik aufzugehen. So drückt sich dann in der Vorsorge weniger ein explizites Misstrauen in die Zuverlässigkeit der Technologie aus, sondern eine generelle Haltung, wonach Technik schlicht fehlbar ist. Das Verfahren wird dann nicht allein deshalb verwendet, weil es Dinge wie Bargeld oder den PIN überflüssig und damit Prozesse einfacher macht, sondern weil diese zwar gefühlt einfacher

[58] Während die befragten Schüler und Videothekenkunden in der Regel über längere, das heißt mindestens mehrwöchige, teils mehrjährige Nutzungserfahrungen verfügen, haben die befragten Supermarktkunden wenig oder gar keine Erfahrung im Umgang mit dem Fingerabdruckscanner. Dass insofern die Erzählungen über die Notwendigkeit von Absicherungen angesichts potentiellen Nicht-Funktionierens durch alternative Verfahren zwischen den einzelnen Anwendungssettings variieren, mag dann auch dem Zeitpunkt der Durchführung der Untersuchung geschuldet sein.

werden, aber man trotzdem nicht davon abhängig ist oder zumindest Unterstützung, etwa durch das Kassenpersonal, erfährt. In diesem Zusammenhang deutet sich auch an, dass von dem Komfortnutzen des neuen Verfahrens zu profitieren nicht bedeutet, eine distinktive Wertigkeit zu kommunizieren (vgl. hierzu Hörning 2001: 44). Die Verwendung des Verfahren gilt den Nutzern, im Gegenteil, mehrheitlich nicht als „objektiviertes Kapital" (vgl. Bourdieu 1983: 191). Vielmehr soll sich seine Nutzung im Gebrauch möglichst unauffällig in den Alltag einfügen, um, wie es Frau Müller, stellvertretend für viele Interviewten, ausdrückt, *„Dinge, die man auf jeden Fall erledigen muss, möglichst unprätentiös erledigen zu können: Bezahlen ((lacht))."* (Petra Müller, Sm). Dies entspricht im Übrigen ebenfalls der Bewerbung des Verfahrens in diesen Anwendungskontexten. Wie Jana Böger (2012) in ihrer Analyse der Darstellungen der Fingerabdrucktechnologie in den Werbematerialien der untersuchten Anwendungskontexte ermittelt, wird das Verfahren eher normalisiert, als dass distinktive, etwa Lifestile-Elemente hervorgehoben würden. Mit einem mitunter postulierten kulturellen Wertbestand technischer Effizienz (vgl. Kapitel 1.1.2.1) durch biometrische Verfahren scheint insofern nicht automatisch auch ein individueller Selbstzweck einherzugehen.

Dass technisches Handeln menschliches Tun für die Nutzer nicht zwangsläufig ersetzt, zeigt sich im Setting Arztpraxis auf einer ganz praktischen Ebene und im Hinblick auf die Gründe, die zur Abschaffung des Systems führten. Der Erwartung des Arbeitsgebers, dass das System der Zeiterfassung bislang eher informell organisierte Kontrollnotwendigkeiten verringere – die Angestellten etwa nicht länger Beschwerden über ungleiche Arbeitszeiten an ihn richten müssen – und daher aus seiner Sicht einen persönlich entlastenden Effekt besitzt, steht der Aufwand gegenüber, der aus der Pflege des Systems resultiert. So wies dieses für viele Mitarbeiter gegen Ende seines Einsatzes zahlreiche ungerechtfertigte Fehlstunden infolge nicht eingetragener Urlaubs- oder Krankenzeiten aus. Konfrontiert dies den Arbeitgeber erneut mit der Beschwerde der Angestellten, entsteht daraus eine Doppelbelastung: Den Arbeitnehmern das Wissen um den Fehler zu versichern und diesen dann auch durch Nachtragungen im System zu ändern:

> „und so viel Fehlstunden (I: Ja.). Dass, dann sag ich denen, ‚Au Mensch, entspann' Sie sich, das stimmt nich', is' auch nich' für irgendwas relevant so'. ‚Ja, es stört mich aber trotzdem, können Sie das nich' mal abstellen?' ((nachäffender Tonfall)), irgendwie so (I: Hm.) ja und das is' dann so, dass dann, je nachdem wie schnell sie dann davon genervt sind, das war auch unterschiedlich, manche die hatten da elf Fehlmeldungen angestaunt." (Michael Clausthal, Arzt)

Scheitert der Versuch, dem Fehler Relevanz abzusprechen – da er bedeutet, die Relevanz des Systems selbst in Frage zu stellen –, entsteht mit den zunehmenden Fehlermeldungen auch ein

Nutzungszwang für den das Zeiterfassungssystem nicht benutzenden Arbeitgeber, nämlich regelmäßig Unstimmigkeiten im System zu beseitigen. Dieser lässt sich jedoch nicht dauerhaft in die Technikbedienung einzwingen und weist das System letztlich als *„zu aufwändig“* aus und beendete die Zeiterfassung in der Praxis.

3.2.1.3 Situative Erfordernisse

Technische Zusammenhänge, kulturelle Alltagspraktiken und Routinen stellen das „Gebrauchswissen“ (Schütz/Luckmann 2003: 157ff.) bereit, mit dem sich häufig der Sinn des Fingerabdruckverfahrens erschließt. Im behördlichen Setting realisiert der entsprechende situative Rahmen die ‚Passung‘, auch dann, wenn die Nutzer mit der Technologie keinen bestimmten oder gar kohärenten Zweck verbinden. Wenn sich also in diesem Zusammenhang auch situative Deutungen von Relevanz für eine Nutzung erweisen, dann lässt sich das Nutzungshandeln der Befragten auch insofern als unterschiedlich motiviert ausweisen, weil dieses Zusammentreffen von technischen Ensembles, Institutionen und Menschen mitunter „soziale Bahnungen“ (Reichertz 2014: 116) kreiert: die Befragten „finden dort typische Motive vor, die geneigt machen, bestimmte Entscheidungen zu treffen, und sie begegnen Anderen, die von ihnen erwarten, eine bestimmte Wahl zu treffen.“ (ebd.)

Nicht alle Befragten im Setting Einwohnermeldebehörde verknüpfen mit dem Verfahren persönlich relevante Zwecke. So folgen viele, für die sich ein konkreter Zweck nicht unmittelbar erschließt, vielmehr der „Orientierungskundgabe“ (Goffman 1974: 184ff.) der Mitarbeiter des Meldeamts, wonach der Fingerabdruck *„zur Sicherheit“* ist, wie der nachfolgende Auszug aus einem Beobachtungsprotokoll illustriert:

> Aus dem Beobachtungsprotokoll Antragstellung Personalausweis Günter Konrad: Herr Konrad, Rentner, ca. 65 Jahre, ehemaliger selbständiger Unternehmer, beantragt einen neuen Personalausweis. Auf den Hinweis des Sachbearbeiters, es dauere ca. drei Wochen, meint er, „erstaunlich, wie schnell das geht“. Er lächelt oft und guckt mich dabei an. Der Sachbearbeiter fragt: „Möchten Sie die Fingerabdrücke speichern lassen?“ Herr Konrad schweigt und guckt mich und den Sachbearbeiter an. Dieser sagt: „Ist ein weiteres Sicherheitsmerkmal“. Herr Konrad sagt daraufhin „ja“ und nickt. Sachbearbeiter: „Der Fingerabdruck wird auch nicht hier, sondern auf einem Chip gespeichert“ Anschließend verweist der Sachbearbeiter auf die Internetnutzung und bittet um die üblichen Unterschriften.

Die Entscheidung, die Herr Konrad ohne Zögern trifft, deutet darauf, dass das eher abstrakte Sicherheitsargument des Behördenmitarbeiters, als kaum hinterfragbare Wertidee, einen geradezu appellativen Charakter (vgl. Kaufmann 2012: 258) entfaltet. Auch wenn Herr Konrad

den Sinn und Zweck der Erfassung von Fingerabdruckdaten selbst eher als diffus erfährt und im Interview erklärt, nicht *„nachvollziehen [zu können], was da sich überlegt wird“*, ist für ihn der Hinweis auf ihren Sicherheits-Hintergrund handlungsrelevant:

> Günther Konrad: „Ja, aber is‘ ja ‘ne sicherheits-relevante Sache, ne, letzten Endes.“
>
> I: „Ja, und das war für Sie“
>
> Günther Konrad ((fällt ins Wort)): „ausschlaggebend, ja, ja. Klar.“
>
> I: „Hatten Sie sich das vorher überlegt, oder war das jetzt spontan oder so?“
>
> Günther Konrad ((fällt ins Wort)): „Nö, das is‘ im Grunde für mich logisch, ne. Da hab‘ ich gar nich‘ drüber nachgedacht, was für logisch is‘ oder was. Sicherheitsrelevant is‘, das akzeptier ich auch gleich.“

Mit der Erkenntnis, dass ein – wenngleich diffuses – Sicherheitsproblem vorliegt, entsteht für Herrn Konrad eine Handlungsaufforderung, der er nachkommt, ohne mehr darüber wissen zu wollen. Der Impuls der Handlung wird allein durch die Rede von Sicherheit in Gang gesetzt, sie wird zur „Konsensrhetorik“ (Lucke 1995: 162). Allerdings erscheint es vielen der Befragten auch nicht als ungewöhnlich, sondern vielmehr typisch, dass eine Behörde für eine Ausweisbeantragung Daten erfragt und speichern lässt. So wird der Zweck einer Technologie wie des Fingerabdrucks im behördlichen Kontext dann auch als selbstverständlich und nicht weiter erklärungsbedürftig angenommen. So meint etwa Herr Zander (Einwo), „*das Angebot mit dem Fingerabdruck […] so eher spontan“* wahrgenommen zu haben, ohne, wie die Beobachtung zeigt, weitere Informationen durch die die Daten aufnehmende Sachbearbeiterin erhalten zu haben. Die Bedeutung einer solchen, eher formalistischen, Routine erweist sich zudem darin, dass es einigen Fällen auch weniger das preiszugebende Datum und die entsprechende Technologie ist, zu der die Befragten ihr Handeln ins Verhältnis setzen, als vielmehr die wahrgenommene Selbstverständlichkeit einer ‚Behördensituation‘. So kann, in anderen Worten, dann auch schlicht der „soziale Anlass“ (vgl. Goffman 2009: 34) motivierend für die Preisgabe der Fingerabdruckdaten sein. Vor allem im behördlichen Setting verbindet sich mit der Aufnahme der Fingerabdrücke in die Ausweisdokumente, trotz der in Kapitel 3.1.1.3 dargestellten Zwecke, dann auch mitunter weniger eine persönliche, als vielmehr eine „hypothetische“ Relevanz (Schütz/Luckmann 2003: 185), das heißt die Zuwendung zum Verfahren erfolgt unmittelbar in der Situation und zumindest vorerst ohne eine explizite Auseinandersetzung. So basieren dann auch eine Reihe der in den Interviews formulierten Zwecke der Technologie auf eher routinemäßig motivierten ‚Sicherheitsvorkehrungen‘, die infolge dieser hypothetischen Relevanzen entstanden sind.

Viele Nutzer beschreiben in den Interviews dann auch eine eher pragmatische Haltung, wenn sie etwa im Interview erklären *„ich nehm‘ das einfach zu Kenntnis und verhalt‘ mich dann entsprechend“* (Günter Konrad, Einwo). Entsprechend bleibt der Fingerabdruck im Prozedere der Antragstellung zuweilen auch nur eine Marginalie, die einfach mitgenommen wird, weil es *„nicht zusätzlich was kostet“*. (Doris Ulmer, Einwo). Wenn diese Befragten in der Regel während der Antragsstellung keine weiteren Fragen stellen, dann vor allem deshalb, weil sie den Behördengang schlicht *„hinter sich bringen“* wollten (Nils Heidrich, Einwo). Als typisch für ein solch gefälliges Hinnehmen stehen die Äußerungen der 40-jährigen Doris Ulmer, denn für diesen *„Schnickschnack“* von Fingerabdruck weiß sie weder konkrete Vor- noch Nachteile zu benennen. Die Beobachtung während der Antragstellung ihres neuen Personalausweises spiegelt diese Bewertung zunächst wider:

> Aus dem Beobachtungsprotokoll Antragstellung Personalausweis Doris Ulmer: Frau Ulmer, ca. 40 Jahre, beantragt einen neuen Personalausweis. Auf die Frage des Sachbearbeiters, ob der Fingerabdruck mit registriert werden soll, meint sie zunächst zögerlich „nein“. Der Sachbearbeiter stutzt ganz kurz und meint dann gleich, es sei „kein Nachteil“ und „ein weiteres Sicherheitsmerkmal“. Daraufhin und ohne weitere Fragen oder andere Äußerungen lässt Frau Ulmer den Fingerabdruck doch erfassen bzw. unterschreibt dies zunächst, da dies der Erfassung vorausgeht. Beim Einlesen der Fingerabdrücke, das ohne weitere Ausführungen seitens des Sachbearbeiters beginnt, ist sie auf den Scanner und das Lämpchen konzentriert. Der Frage nach dem Interview stimmt sie leicht zögernd zu und wir gehen nach kurzer Absprache in das Geschäftszimmer.

Gibt Frau Ulmer erst mit dem Nachhaken des Sachbearbeiters, wonach eine Speicherung der Fingerabdrücke nicht zu ihrem Nachteil, aber ein weiteres Sicherheitsmerkmal sei, ihr Einverständnis zur Aufnahme der Fingerabdrücke, dann ist für dieses, anders als etwa bei Herrn Konrad, weniger das Sicherheitsargument ausschlaggebend, denn *„eigentlich war‘s mir egal“*. Vielmehr ist es die wiederholte Aufforderung, gewissermaßen die „soziale Sanktion“ (vgl. Goffman 1974: 138ff.) auf ihr Zögern, der sie sich fügt. Im Interview erklärt sie dann auch: *„dann hab‘ ich gedacht, ‚na ja, warum nich‘? Also, wenn's jetzt nich‘ zusätzlich was kostet“*. Erklären lässt sich dieses Einverständnis dann damit, dass eine zunächst neue, nicht durch Gewohnheitswissen abgedeckte Situation – dass für den Personalausweis eine Aufnahme der Fingerabdrücke möglich ist, war ihr nicht bewusst – so in eine aktuelle Relevanzstruktur überführt wird, nämlich einen Pflichttermin bei der Behörde ohne weiteren Aufwand zu überstehen:

> „So, also das is‘ halt so, also es is‘ halt Usus, man hat ‘n Personalausweis ((lacht)), so, und wenn der abläuft, dass man halt ein‘ Neuen machen, also braucht, so.“ (Doris Ulmer, Einwo).

Dieser Anpassungszwang ist für Frau Ulmer unproblematisch, weil sie aus ihrer nachträglichen Entscheidung keinen finanziellen Nachteil erwartet und sich ihr Verhalten dann mit einem generellen Zwang, der sich aus der Ausweispflicht ergibt, erklärt. Gemessen an ihrem eher geringen Interesse an der Aufnahme der Fingerabdrücke in den Ausweis erfordert dies für sie auch kein größeres Engagement in der Auseinandersetzung mit dem Sachbearbeiter.

Es zeigt sich aber auch noch weiterer Zusammenhang zwischen der Wahrnehmung der sozialen Situation und dem Engagement, der sich aus den in ihr angelegten Forderungen nach spezifischer Aktivität ergibt. Denn vor allem in Situationen im Kontext institutionell-organisatorischer Verfahren herrschen, erstens, nicht nur andere Interaktionsregeln, sie unterscheiden sich von einer Alltagskommunikation, zweitens, auch dahingehend, dass hier „Aktivitätsrechte“ (Steuble 1983: 179f.) der Beteiligten in besonderer Weise (bzw. ungleich) verteilt sind, die sich aus der spezifischen Struktur jener Situationen ableiten. Heritage (2004 224f. mit Bezug auf Drew and Heritage 1992) zufolge zeichnet sich die institutionelle Interaktion nicht nur dadurch aus, dass die Teilnehmer bestimmte Ziele haben, die mit ihrer Rolle in dem jeweiligen Setting verknüpft sind. Es liegen auch Beschränkungen dahingehend vor, was als erlaubter Beitrag für die verhandelte Angelegenheit innerhalb des Rahmenwerks und seiner Prozeduren gilt. Vor diesem Hintergrund spielt bei Antragstellern im Einwohnermeldeamt auch der wahrgenommene soziale Druck für Fragen der Akzeptanz eine Rolle, wenn die vermeintlich informellen Regeln in einer bekannten Situation nicht durchbrochen werden sollen, wie dann auch die nachfolgende Passage aus dem Interview mit Angelika Wilde (Einwo) verdeutlicht, die sich zwar gegen eine Aufnahme der Fingerabdrücke in den Personalausweis entschied, im Interview aber ausführlich die Vor- und Nachteile diskutiert:

> I: „Mmh ((bestätigend)). Angenommen, die Anmeldesituation hätte jetzt etwas länger gedauert, hätten Sie diese Fragen noch gestellt? Was meinen Sie?“
>
> Angelika Wilde: „Nee, ich glaube nicht. Weil, dort, das is‘ ja ‘ne andere, das is‘, man hat eine Nummer, man hat so einen gewissen, ja, wie soll man sagen, so Rahmen, wo man auch sagt, so schnell rein, es sitzen draußen welche, man hört dann schon ‚Ach ich hab‘ die Nummer, dann komm ich dann‘ und so, also, das is‘ so eingepackt. Man hat nich‘ das Gefühl, man setzt sich hin, er erzählt etwas, sagt etwas da drüber und dass man die Zeit hätte, noch mal so ausführlich das Für und Wider abzuwägen. Wenn man eben spontan sich entscheiden muss. Weil, dann entscheidet man sich eigentlich für das, ich hab‘s nich‘ gehabt, und gut is‘. (I: Ja) Also, da wird, wird diese kurze Diskussion vielleicht mit Ihnen, warum es wichtig wäre und dann meins, mein Für und Wider, die Zeit, denk ich mal, hat man vom Gefühl her da nicht. (I: Ja) Weil man ja immer weiß, da sitzen ja draußen auch welche, die sagen ‚Hmh, Mensch, braucht die lange‘, und ‚da sind schon drei raus, nur die is‘ noch nich‘ raus“ ((schmunzelt)). So, also man hat da nich‘ diese Ruhe. Ne?“

Mit dem Verweis auf den situativen *„Rahmen“* eines Behördenganges, in den die Fingerabdruckgabe eingebettet oder *„einpackt“* ist, deutet Frau Wilde auf Schicklichkeitsregeln, die die Möglichkeiten vorgeben, was in der behördlichen Situation typischerweise kommunizierbar oder im Handeln möglich ist und was in diesem Sinne von beiden Interaktionspartnern regelmäßig erwartbar ist. Obwohl sie im Interview ein Bedürfnis nach weitergehenden Informationen zu Sinn und Zweck der Fingerabdrücke bekundet, das sie auch schon während der Antragstellung verspürte, hatte sie nicht das Gefühl diesbezüglich weitergehende Fragen auch stellen zu können. Auch angesichts der öffentlichen Situation, in der andere Wartende sozial kontrollierend auf ihr Bedürfnis nach ausführlicherer Diskussion mit dem Mitarbeiter einwirken, verbirgt sie stattdessen ihre Ungewissheit und reduziert ihr Engagement aus ihrer Sicht sozial adäquat. Folglich können Entscheidungen für oder gegen die Aufnahme der Fingerabdruckdaten in den Personalausweis auch dadurch motiviert sind, zu vermeiden, sich dem sozialen Anlass gemäß situativ nicht ungemessen zu verhalten, weil bereits die Frage nach dem ‚Warum‘ die Grenzen der gebotenen Höflichkeit überschreiten.

Die Übernahme einer situationsadäquaten Rolle und ein daran ausgerichtetes Verhalten, das auch für die Beobachterin persönliche Befindlichkeiten verhüllt – ein Hadern war Frau Wilde nicht anzumerken –, kann dann dazu führen, dass auch ein ausdrückliches Unbehagen, das sich für manche Befragte mit der Fingerabdruckgabe verbindet, in den Regeln des bürokratischen Settings verschwindet. Die erzwungene Einwilligung zur Speicherung der Fingerabdruckdaten in den Reisepass von Herrn und Frau Petersen – beide sprechen sich im Interview ausdrücklich gegen die Erfassung der Fingerabdruckdaten aus –, deutete sich der Beobachterin wohl in der versteinerten Mine von Herrn Petersen an, wurde aber gleichwohl nicht thematisch. Im Interview hingegen bringen beide ihre kritische Haltung zum Fingerabdruck nicht nur zum Ausdruck, sondern erklären auch ihre Zurückhaltung trotz offenbar starker Emotionen in der Situation:

> Frau Petersen: „Schlimm. Ja, und ich empfand das schlimm, schlimm. Weil es so weit is‘, und dann der Fingerabdruck ((lacht)) is‘ noch ein bisschen mehr, ne? Doch. Das gehört zusammen. Der Fingerabdruck und dieser Fragebogen. Für mich war‘s ‚Oh‘. (I: Mmh). Ja.“
>
> Herr Petersen: „Nur, der Mitarbeiter hat seine Pflicht getan, an dem is‘ nichts auszusetzen.“
>
> Frau Petersen: „Absolut, ne.“
>
> Herr Petersen: „Er muss das durchführen, was ihm aufgetragen wird. Ne?“

Frau Petersen ist sowohl im Besitz der deutschen als auch der französischen Staatsbürgerschaft und musste aus diesem Grund bei der Reisepassbeantragung eine Erklärung zur Staats-

angehörigkeit ausfüllen. Das Unbehagen von Frau Petersen darüber, als Bürgerin mit doppelter Staatsbürgerschaft offenbar besonderen Kontrollprozeduren ausgesetzt zu sein, blieb also deshalb ‚unsichtbar', das heißt privat, weil das Personal gegenüber persönlichen Einwänden immunisiert wurde. Ein solches Management des Selbst zeigt sich auch beim Ehepaar Oppermann, die, wie sie erklären, sich zwar bereits vor dem Behördentermin zur Fingerabdruckabgabe in den Reisepass und den Personalausweis entschieden und ausdrückliche Vorteile damit verknüpfen, gleichwohl diesen als Zwang interpretieren, gegen den man sich aber weder *„wehren"*, noch ihn in der behördlichen Situation verhandeln könne:

> Rüdiger Oppermann: „Das kann man natürlich nich' machen, wenn man dorthin geht und beantragt den, den Reisepass, dass man sacht ‚Nö, also da geb' ich jetzt nich' meinen Fingerabdruck. Das mach' ich nicht'. Dann sagt die ‚Auf Wiedersehen, gehen Sie'. (I: Ja.) Wenn einer sagt, ‚davon hab' ich ja noch gar nichts gehört'."
>
> Veronika Oppermann: „Ja, gut, wir hatten ja gar keine Chance, insofern."
>
> Rüdiger Oppermann: „Ne, aber wir woll'n ja auch mit der Dame da nich' diskutieren."
>
> Veronika Oppermann: „Ne. Die kann da nix für, die is' Ausführende"
>
> Rüdiger Oppermann ((unterbricht)): „Die sagt auch nur ‚Ich mach hier meine Pflicht.'"
>
> Veronika Oppermann: „Unter, die machen ihren Job ((lacht)), da bringt das nix. Wenn, dann müssten wir mit unserem politischen Vertreter darüber reden, ne."

Das Ehepaar Oppermann, welches das Fehlen eines partizipativen Entscheidungsprozesses zur Herstellung von Sicherheit bemängelt, hat für sich also bereits im Vorhinein eine Situationsdefinition aufgestellt und Widerständigkeiten aus dem Schema ‚Beantragung von Ausweispapieren' ausgeschlossen. Diese Definition forciert dann eine compliance in der persönlichen Begegnung mit der Vertreterin des Systems.

Entsprechende Situationsrahmungen werden auch dann durchgehalten, wenn sich Unstimmigkeiten ergeben. Frau Böttcher, die, wie bereits in Kapitel 3.1.1.3 dargestellt, das zunächst Unvertraute der Fingerabdruckabgabe mit der Notwendigkeit ihr *„administratives Ich"* im Personalausweis zu ergänzen, normalisiert, erfährt während des Einlesens ein – für den Beobachter nicht wahrnehmbares – Unbehagen, welches durch die „kriminologische Assoziation" (Breitenstein 2002: 40) des Verfahrens, das heißt den Bezug zu seiner traditionellen polizeilichen Verwendung, evoziert ist. Im Interview nach dem Gefühl befragt, das sie empfand, als sie ihren Finger auf den Scanner legte, antwortet sie spontan:

> Greta Böttcher: „Naja, war Verbrecheralbum, ne." ((lacht etwas))
>
> I: „Verbrecheralbum sagen Sie." ((lacht))
>
> Greta Böttcher ((lacht)): „Wie man so sagt, ne."

I: „Ja, das war Ihr erster Gedanke danach."

Greta Böttcher. „Ja, das ist, ne, ((unverständlich)) Nur so'n Schnack."

Obwohl Frau Böttcher diese Assoziation der Kriminalisierung als für sie Typisches der Fingerabdrucktechnologie umgehend als einen *„Schnack"*, als mitunter gebräuchliche, gleichwohl aber leere Rede disqualifiziert, regt es sie dazu an, die situativen Bedingungen der Fingerabdrucknahme in den Blick zu nehmen. Rekurriert sie hierzu auf die Bedeutung der Ausweispapiere, zu denen die Fingerabdrücke *„gehören"*, wirft sie dann erstmals die Frage der Freiwilligkeit ihrer Abgabe auf, die ihr offenbar in der Situation nicht in den Sinn gekommen ist: „*Das gehört ja zu meinem Ausweis dazu. Kann ich mich eigentlich wehren oder sagen, ich möchte das nicht mit meinem Finger? Ja, das kann ich, ne? Ja."* Mit der ausdrücklichen Aufforderung an den Interviewer, zu klären, ob sie die Daten hätte preisgeben müssen, stellt sie also die Bedingungen in Frage, auf denen sie ihre Entscheidung gründete. Hier handelt sich es um eine Akzeptanz unter anderen Voraussetzungen als von der Befragten angenommen.

3.2.2 Ambivalenzmanagement

Angesichts unterschiedlichster Funktionen und trotz zahlreicher praktischer Vorteile erweist sich das Fingerabdruckverfahren, wie in Kapitel 3.1.2 dargestellt, für die Befragten mehrheitlich als eine ambivalente Technologie. Anders als ursprünglich vermutet, ist diese Ambivalenz aber nicht das Ergebnis von ‚öffentlich' in den Anmeldesituationen verhandelten Bedeutungen. Die Interviewten thematisieren (Un-)Sicherheit und Überwachung vielmehr als individuelle Spannungsfelder, das heißt als Teil eines politischen Diskurses, zu dem sie sich mit ihren persönlichen Ansichten ins Verhältnis setzen. Als zentrale Bezugspunkte erweisen sich dabei Vorstellungen von der Sicherheitsleistung des Fingerabdrucks und mitunter daraus resultierende, imaginierte Unsicherheitsszenarien. Für die weitere Einschätzung der Akzeptanzbedingungen zeigt sich, neben der Bedeutung sozio-technischer Rahmungen und situativer Deutungen dann auch eine Differenz, mitunter sogar eine Ambivalenz zwischen tatsächlicher Fingerabdruckabgabe einerseits und kritischen Räsonnement andererseits. Der Vergleich der Interviews sowohl zwischen, als auch innerhalb der Anwendungssettings, zeigt, dass es den Nutzern in unterschiedlichem Maß gelingt, die mit der Technologie verbundenen Ambivalenzen für sich aufzulösen. Zwei Bedingungen sind dafür zentral: zunächst eine niedrigschwellige Bewertung der anfallenden persönlichen Daten. Dabei handelt es sich weniger um eine individualisierte Risikowahrnehmung im Sinne eines ‚optimistic bias', als vielmehr um eine kontextuell variable ‚Normalisierungstendenz', die sich in einem Zusammenhang damit be-

schreiben lässt, welche Bedeutung und mithin welcher Wert dem Datum Fingerabdruck in unterschiedlichen Anwendungssettings und damit verknüpften Verwendungsszenarien zugeschrieben wird. Zweites lässt sich zeigen, dass der natürliche Zwang des Routinewissens über gewohnte Strukturen das Handeln der Nutzer nicht ausschließlich determiniert, sondern die Risikoeinschätzung der Datenverwendung vielmehr in einem ausdrücklichen Vertrauen in den Fingerabdruckabnehmer neutralisiert wird.

3.2.2.1 Relative Privatheit und Vorstellungen kontextueller Integrität

Wie etwa auch Zurawski (2011: 510) für die Praktiken der Verwendung von Kundenkarten herausgearbeitet hat, erweist sich das Thematisieren der Fingerabdrucktechnologie als narrativer Rahmen für Fragen von Privatheit und Datenschutz, die, wie beschrieben, in den beobachteten Anmelde- und Registrierungssituationen nicht aufgeworfen wurden. Demgegenüber werden in den Interviews gleichwohl lokale Praktiken der Datenpreisgabe in Verbindung zu (globalen) Datenströmen gebracht und die Auseinandersetzung mit der Technologie regt dann auch zur Thematisierung gesellschaftlicher Diskurse an. So sind den Befragten etwa, auch wenn sie die Speicherung nur eben ‚mitgenommen' haben, Datenschutzfragen durchaus gegenwärtig. Die heutige und aus ihrer Sicht technikbedingte Unbefangenheit der Datenpreispreisgabe betrachtet etwa Frau Ulmer kritisch:

> „heutzutage läuft jeder mit'm Apple rum und is' rund um die Uhr online, und postet allen möglichen Kram, und früher haben sie demonstriert gegen Datenschutz und heute steht jeder Pups auf, auf irgendso'ner Seite." (Doris Ulmer, Einwo)

Obzwar die von den Befragten geäußerte Ambivalenz regelmäßig auf der von allen Befragten geteilten Überzeugung basiert, dass die Methode des Fingerabdruckverfahrens zwar eine objektive Identifizierung ermöglicht, es mit Blick auf das potentielle Hinterlassen des Fingerabdrucks im Alltag (als einer leibhaften Körperlichkeit) aber auch zum riskanten Indiz für persönliches Handeln geraten kann (vgl. Kapitel 3.1.3f.), stellt der Fingerabdruck selbst für die Frage der Privatheit, trotz seines körperlichen Bezugs, für viele Befragte nur ein Datum unter anderen dar. Macht man Privatheit also zunächst daran fest, was Personen als besonders schützenswert begreifen, dann lassen sich in den Interviews so unterschiedliche Informationen wie Telefonnummern, Adressen oder regelmäßig Kontodaten ausmachen und mitunter auch Angelegenheiten, die nicht als Daten per se erscheinen. So erklärt ein Interviewter in der Behörde etwa, dass ihm die Sicherung seiner Doktorarbeit auf dem PC als wesentlich vordringlicher erscheint, als die des Fingerabdrucks in seinem Reisepass:

> „Ja, zum Beispiel Kontodaten. Oder was ich so am Telefon mach‘ oder meine Sachen, was auf meinem Rechner, an dem meine Doktorarbeit gespeichert sind, bearbeiten, zum Beispiel so was. Ja. Das würde mir wesentlich mehr Schmerzen denn wie beim Fingerabdruck.“ (Nico Heidrich, Einwo).

Privatheitsverletzungen bestimmen sich folglich nicht per se aus der Intimität eines Datums (zu Privatheit als Intimität vgl. Innes 1992), sondern auch die Verwendung von Daten, wie etwa Adressen oder Kontodaten, können Privatheit verletzen. In diesen Vergleichen zeichnen sich in Anlehnung an Goffman (1974) folglich, zum einen, unterschiedliche Vorstellungen von ‚Privatheitsterritorien‘ ab, weil etwa die Preisgabe der Telefonnummer bedeuten kann, dass *„lästige“* Telefonanrufe (Petra Müller, Sm) in den persönlichen Wohnraum eindringen, in dem man aber ungestört bleiben will bzw. die Verwendung der privaten Telefonnummer zu Geschäftszwecken des Ehepartners die Möglichkeit einschränkt, im eigenen Heim dauerhaft eine private Rolle für sich zu beanspruchen. Aber auch der Inhalt eines Gesprächs selbst kann als privat, weil intim gelten, der, wie bei Herrn Heidrich, entsprechende Teilnahmeberechtigte an diesem „Gesprächsreservat“ (Goffman 1974: 69) voraussetzt. Der Wert des Fingerabdrucks wird, zum anderen, erst durch die als persönlich wichtig erachteten Daten selbst bestimmt. Dies zeigt sich darin, dass eine Fingerabdrucknutzung regelmäßig dann ausgeschlossen wird, wenn sie als Risiko für das finanzielle Besitzterritorium wahrgenommen wird. Dies korrespondiert dann auch mit einer Einschätzung von Cole und Pontell (2006: 128) zum Narrativ des Identitätsdiebstahls, wonach der Wert des Objektes – die gestohlene Identität – generell geringer ist „than the value of goods whose security is endangered by the theft (bank accounts, credit ranting, etc.)“. In der Tat erfährt der Fingerabdruck in Verbindung mit den Kontodaten etwa bei der Verwendung im Supermarkt, im Vergleich zum behördlichen Setting, dann eine vergleichsweise höhere Bedeutung, wie auch Herr Heidrich (Einwo) weiter ausführt:

> „Nee, da hab‘ ich ja ‘n ernstes, da is‘ dat Ding, da is‘ der Fingerabdruck deutlich mehr Wert. Wenn man mit dem bezahlen kann. Also, wenn jetzt irgend‘n Hansel in Indien meinen Fingerabdruck runterladet, is‘ mir eigentlich egal, sag‘ ich jetzt mal. Wenn ich jetzt mit dem Fingerabdruck bezahlen kann, dann is‘ das ja quasi wie ‘ne Kreditkarte. Das wär’ ja blöd, ja? Das würd‘ ich eigentlich schon vermeiden.“

Eine Datensammlung in der Behörde wird dann gegenüber dem hoch eingeschätzten Risiko des Geldverlusts im Supermarkt als eher unproblematisch bewertet. Es werden aber nicht nur die mit dem jeweiligen Anwendungskontext verbundenen ‚realen‘ Risiken verglichen, sondern auch die vorgestellten Prozesse im Hinblick auf die Kombinierbarkeit von Daten. Dies gilt sowohl im Hinblick auf die jeweils vorgestellten Nützlichkeiten – in der Behörde etwa zum Zwecke der Kriminalitäts- und Terrorismusprävention – als auch mit dem Blick auf potentielle Überwachungsrisiken. In diesem Zusammenhang zeigen sich dann auch Deutungsunter-

schiede dahingehend, dass der Wert des Fingerabdrucks mit dem jeweiligen Anwendungssetting variiert, in anderen Worten damit, welche Daten anfallen und auch was mit ihnen in Kombination gemacht werden könnte. Erscheint ein Anwendungssetting in diesem Sinn als ‚wichtig', dass über die Bedeutung von Daten *„nachgedacht"* wird (Julia Franke, Vid), erfährt auch die Technologie eine besondere Bedeutung: *„man denkt darüber nach"* (ebd.). Ausgehend von dieser kontextuellen Wichtigkeit im Hinblick auf ein persönliches Risiko lehnen etwa die Kunden der Videothek mehrheitlich die Nutzung des Fingerabdrucks im Supermarkt ab. Sie gehen davon aus, dass damit ein exaktes Profil über das Einkaufsverhalten und somit auch über den Lebensstil erstellt werden könnte. Demgegenüber erscheint die mit dem Fingerabdruck assoziierte Speicherung der Leihhistorie der Filme als nebensächlich und harmlos und die Interviewten fühlen sich, selbst wenn diese Informationen Dritten zugänglich gemacht werden würden, nicht ‚festgelegt':

> Corinna Meier (Vid): „Deswegen fand ich's in der Videothek nicht so schlimm, nee. (I: ok) Bei 'ner Bank, glaube ich, weiß ich nicht, ob ich das wollen würde oder, ich weiß auch nich'. Bei der Videothek, das find ich so irrelevant. Also."
>
> I: „Hast du das irgendwie schon gehört mit der Bank, dass man das, das man das irgendwie vielleicht machen könnte oder wie kommst du jetzt darauf?"
>
> Corinna Meier: „Nö, is' mir jetzt nur so eingefallen, als Seriöseres. Da hängen ja jetzt auch sensiblere Daten hinter, über die Bankdaten kriegt man ja viel mehr über ein' Menschen raus als über so 'ne Videotheken-Information. Ich glaub, das fänd ich schon sensibler, ja."

In diesen Unterscheidungen, ebenso wie angesichts der von den Befragten entfalteten, mitunter diffusen, Missbrauchsszenarien (vgl. Kapitel 3.1.2), wird dann auch deutlich, dass theoretische Differenzierungen etwa zwischen informationeller und dezisionaler Privatheit (Rössler 2001: 25) im empirischen Material keine eindeutige Entsprechung finden. So geht es bei der informationellen Privatheit um den Anspruch „vor unerwünschtem Zugang im Sinne eines Eingriffs in persönliche Daten über sich geschützt zu werden" (ebd.). Hingegen liegt der dezisionalen Privatheit das Verständnis zu Grunde, dass es Lebensbereiche gibt, die einen anderen nichts angehen – sie also dem Schutz vor Einspruch in das individuelle Verhalten unterstehen (ebd.: 144). Mit Blick auf die unterschiedlichen Anwendungskontexte realisiert sich mitunter aber das eine erst aus dem anderen. Und auch das Konzept Privatheit selbst erscheint als eine relationale Kategorie – nicht nur dahingehend, dass was dem einen Nutzer als privat erscheint, ein anderer dem öffentlichen Blick nicht offenbaren möchte. Angesichts individueller Praktiken des Privatheitsmanagements – also Entscheidungen darüber, welche Daten man wo (nicht) preisgibt – ist auch Sichtbarkeit nicht per se problematisch und so erscheint auch eine verallgemeinerbare Grenzziehung zwischen dem Verständnis von öffentlich und privat als

schwierig. Dies zeigt sich auch darin, dass in der Videothek, ein Setting, das sich sowohl als privater Freizeitbereich als auch als öffentlicher, weil gesetzlich reglementierter, Kontext darstellt, gleichwohl erwartet wird, dass hier entstehende Informationen das Setting nicht verlassen, selbst wenn die Daten nicht so *„sensibel“* (Corinna Meier, Vid) sind.

Der Privatheitsbegriff, wie ihn Beate Rössler (2001) entfaltet und in dessen Mittelpunkt die Autonomie des Einzelnen steht, „die nur möglich ist unter Bedingungen geschützter Privatheit“ (ebd.: 137), und der eng an den Begriff der Kontrolle angelehnt ist, korrespondiert stark mit dem Recht der informationellen Selbstbestimmung. Danach bezieht sich Privatheit auf die Möglichkeiten des Einzelnen, zu wissen, wer welche Informationen über die eigene Person und die Lebensumstände erhält:

> „als privat gilt etwas dann, wenn man selbst den Zugang zu diesem ‚etwas‘ kontrollieren kann. Umgekehrt bedeutet der Schutz von Privatheit dann einen Schutz vor unerwünschtem Zutritt anderer.“ (ebd.: 23)

Aus einer Außenperspektive lassen sich auf diese Weise Privatheitsverletzungen beschreiben, etwa das ungewollte Ausspähen von Kommunikation und im Hinblick auf ihre Konsequenzen problematisieren. Gleichwohl bedeutet für die Befragten nicht jedes Verletzen der Privatsphäre einen Verlust an Autonomie, wie etwa der regelmäßige Hinweis auf die Bedeutung der Kontodaten zeigt. Und regelmäßig bleibt zudem für eine Reihe der Befragten die Frage offen, wie eine Kontrolle über die eigenen Informationen eigentlich gelingen kann. So weisen diese daraufhin, dass eine mutmaßlich nicht-intendierte Datenverwendung normal ist, weil den Befragten das Handeln der Akteure, die Zugriff auf die Daten erhalten, als unberechenbar erscheint bzw., wie exemplarisch der 25-jährige Carsten Welzer (Einwo) ausführt, aufgrund der Verwertbarkeit der Daten, Kontrolle an ihre gesetzlichen Grenzen stößt:

> I: „Also, du hast am Anfang gesagt, verschiedene Sachen gehen in Richtung Überwachungsstaat, und“
>
> Carsten Welzer ((unterbricht)): „oder um die technischen Möglichkeiten.“
>
> I: „Gut, da muss man unterscheiden, das is‘ richtig. Und wenn du jetzt sagst, ökonomische Interessen sind noch brisanter, also das ist, da unterscheidest du nochmal, ob das jetzt Staat ist oder Privatwirtschaft?“
>
> Carsten Welzer: „Richtig. Denn es ist definitiv ökonomisch.“
>
> I: „Und der Unterschied ist für dich aber diese wirtschaftliche Interessen, oder gibt‘s noch andere?“
>
> Carsten Welzer: „Wirtschaft ist ja, sind ja hauptsächlich Privatpersonen, die sich nie, vor nichts rechtfertigen müssen.“

Der undurchschaubaren Überwachung steht die eigene Sichtbarkeit gegenüber. Weil die die eigene Sichtbarkeit herstellenden Prozesse selbst unsichtbar bleiben, findet die Selbstbestim-

mung über die eigenen Daten ihre Grenzen gerade dort. Stehen für die Befragten nun in der Tat unterschiedlichste Akteursfiguren für die Bedrohung: *„Betrüger“, „Hacker“*, „*der Staat“*, *„Dritte“* – mitunter *„Jeder“* könnte Interesse an den Daten haben – beschreiben sie ein Missbehagen, mit dem die Grenze zwischen Datensicherheit und Datenschutz innerhalb der „surveillance assemblage“ (Haggerty/Ericson 2000) für sie unklar wird, weil mit den multiplen Risiken Zurechenbarkeiten diffus werden, wie etwa auch Herr Hildesheimer (Einwo) erklärt:

> I: „Außer jetzt die Behörden hier oder an der Grenze, wer könnte da noch Interesse an solchen Daten haben?“
>
> Thorsten Hildesheimer: „Alle“ ((spontan)).
>
> I: „Alle sagen Sie?“
>
> Thorsten Hildesheimer: „Alle. Durchgängig. Da wird Geschäft mit gemacht, is‘ dann egal wo, egal was. Man hört es, man sieht es, man kriegt es vielleicht sogar mit. Ich hab‘ einmal ‘ne Anfrage gemacht beim [Name eines Reiseanbieters], bei meinem Reisegesellschaft, seitdem steh‘ ich bis zur Hüfte in Werbepapieren. Also, irgendwo, phhh, und wenn ich dann irgendwann vielleicht utopisch vielleicht oder wat, aber ich nehm‘ mein‘ Fingerabdruck und drück den auf mein‘ Rechner rauf, der liest den, ohne, das is‘ denn automatisch meine Adresse und hin und her und tüdelüt, also, is‘ utopisch, geb‘ ich gerne zu, aber ((stockt kurz)) es wäre dann zuzuordnen. Da hätt‘ ich irgendwie, da kann, Schindluder mit getrieben werden, denk ich mal.“

Impliziert vor diesem Hintergrund die freiwillige Preisgabe biometrischer Daten einen Kontrollverlust, heißt dies nun gleichwohl nicht, dass Ansprüche auf Privatheit aufgegeben werden – sei es, weil ein Zwang zur Datenpreisgabe vorliegt, wie etwa im Fall von Herrn Hildesheimer oder dem Ehepaar Petersen bei der Beantragung des ePasses, oder weil der Datenmissbrauch ubiquitär erscheint. Eine Aufnahme der Fingerabdrücke in den Personalausweis etwa würde Thorsten Hildesheimer ablehnen, da er mutmaßt, dass dieses *„nationale“* Dokument von der Polizei dazu benutzt werden könnte, die Daten unabhängig von Verdachtsmomenten auszulesen, um *„Bewegungsprofile“* zu erstellen, also der Informationsfluss unangemessen ausgeweitet werden könnte.

Wird regelmäßig ein „Privacy Paradox“ (Acquisti/Grossklags 2004) beklagt, wonach ein kommuniziertes Interesse an Privatheit sich nicht im Handeln der Bürger widerspiegele, müsste sich mit der Wahrnehmung unkontrollierbaren Informationsverlustes im Hinblick auf die Idee der informationellen Selbstbestimmung zumindest im Kontext von Freiwilligkeit ein Handeln zeigen, dass sich die Nutzer bewusst diesen Risiken aussetzen, wenn sie ihre privaten Daten der Öffentlichkeit preisgeben. Allerdings deuten auch Haltungen von Befragten, die den Fingerabdruck scheinbar passiv ‚mitgenommen‘ haben, das heißt Haltungen, die auf den ersten Blick zwischen Fatalismus und Resilienz gegenüber potentiellen Risiken des informationellen Kontrollverlusts zu oszillieren scheinen, gleichwohl darauf hin, dass Ansprüche auf

Privatheit ihren Ausdruck auch in Konventionen der Datenverwendung finden. Diese bestimmen dann auch, was (nicht) als Verletzung und damit als Übergriff empfunden wird, mithin wo Vulnerabilität entsteht und wo nicht. Werden von den Befragten regelmäßig etwa ‚facebook' oder auch das ‚Onlinebanking' zu Bezugspunkten einer problematischen ‚öffentlichen' Präsenz, die sie als riskant, weil in ihren Konsequenzen als unabsehbar wahrnehmen, setzen sie diese vielfach von der eigenen, etwa der behördlichen und anlassbezogenen Datenabgabe ab und geben damit dann Vorstellungen von der Legitimität der Datenverwendung zu erkennen:

> „Also, ich finde, das is' irgendwie so öffentlich und irgendwie bei der Polizei, wenn die irgendwie gezielt jemanden suchen und man muss da hin und Fingerabdrücke abgeben oder die suchen 'ne irgend'n Verbrecher oder so, dann find ich das noch mal irgendwie anders." (Doris Ulmer, Einwo)

Der Vergleich zwischen vielfältigen Formen der Datenpreisgabe, der Ubiquität unerwünschter Datenverwendung oder unterschiedlichen Settings, in denen der Fingerabdruck zur Anwendung kommt, wird dann auch zur, zwischen den Befragten variierenden, Grenzziehung zwischen öffentlich und privat und zum Maßstab dafür, was als (un-)angemessene Datenverwendung gilt. Frau Ulmers Annahme, dass die bei der Meldebehörde erfassten Fingerabdrücke gegebenenfalls zu Strafverfolgungszwecken genutzt würden, erzeugt bei ihr lediglich ein diffuses Unbehagen, das sie im Resümee des Interviews dann auch für sich rationalisiert: *„ich denk', na gut, ich hab' mir ja nichts zu Schulden kommen lassen, und warum nich'"*. Die Vorstellung, dass sich Betroffenheiten nur für diejenigen realisieren, die sich ‚schuldig' machen, erlaubt es ihr nicht nur, diesem Unbehagen selbst nicht weiter nachgehen zu müssen, sondern mit dieser vorgestellten Regel der Datenverwendung schließt sie eine eigene riskante Betroffenheit durch weitergehende Kontrolle aus.

So lassen sich Bedingungen der Akzeptanz auch an Vorstellungen der Befragten an kontextuell etablierten Regeln der Datenverwendung festmachen. In diesem Zusammenhang erweist sich gerade die Variabilität sozialer Regeln von Relevanz, mit denen in unterschiedlichen Kontexten unterschiedliche „symbolische Territorien" (Goffman 1974: 68.) respektiert werden, als akzeptanzrelevant. So kann es, auf der einen Seite, als angemessen erscheinen, den Fingerabdruck im bekannten behördlichen Setting zum Zwecke der Versicherung der Identität im Falle einer polizeilichen Kontrolle oder als Beitrag zur Terrorismusbekämpfung oder Strafverfolgung preiszugeben. Die potentielle Verfügbarkeit über Gesundheitsdaten hingegen wird regelmäßig, und wie nachfolgend der 70-jährige Karl Bauman (Sm) ausführt, zum exemplarischen Fall von Grenzziehungen bei der Datenpreisgabe und -verwendung.

> „Ich bin, bin auch, also mein‘, meine Gesundheitsdaten, die hätt‘ ich an sich auch gerne unter Verschluss. Das geht an, das geht mich was an und meinen Arzt. Und sonst niemanden. Das ist genauso wie mein Bankkonto, das geht auch mich was an und die Bank und meine Frau. Aber sonst auch niemanden. Also das sind so, sind so Bereiche, die, da würd‘, da guck ich immer, dass ich die möglichst abschirme.“

Wenn Befragte also Vorstellungen von sozialen Normen des Privaten äußern, mit denen sie entsprechende Bereiche für sich reklamieren, die unzugänglich für Einmischungen Dritter sein sollen, dann korrespondiert dies mit dem Konzept der kontextuellen Integrität, das Helen Nissenbaum (2011, 2004) vorgelegt hat, und das sich primär an jenen Intuitionen orientiert, die darüber Auskunft geben, was in spezifischen Situationen als ein angemessener Umgang mit Privatheit gilt und was nicht. Das von den Befragten formulierte Recht auf den Schutz der Privatsphäre ist danach weder ein Recht auf Geheimhaltung, noch eines auf Kontrolle (ebd.). Für Fragen der Akzeptanz konstituiert sich die Bedeutung von Privatheit so entlang der Frage, wer, zu welchem Zweck, welche Daten einfordern und verwenden darf und woraus sich dann Anforderungen an spezifische Vertraulichkeiten, als einem Schutz des Privaten (vgl. Endreß 2001: 168), ergeben. Erst mit Blick auf die jeweils etablierten Regeln des Informationsaustausches generieren sich also Vorstellungen davon, was als eine Übertretung wahrgenommen wird. Da Nissenbaum (2011) zufolge privat nicht nur das ist, was als intim gilt, sondern Privatheit auch in der Öffentlichkeit verletzt werden kann, konstituieren sich Verletzungen entlang „sozialer Rahmen, informationeller Normen“, und damit auch in Abhängigkeit von den „jeweiligen Rollen des Gegenstands, des Senders (der der Gegenstand sein kann) und des Empfängers dieser Information sowie [den] Grundsätze[n], die für die Übertragung der Information von Sender zu Empfänger gelten.“ (ebd.: 54) Angesichts der spezifischen Situiertheit lokaler Praktiken der Datenpreisgabe lässt sich diese dann auch nicht als ein simpler „trade-off“ beschreiben. Ob sich die Befragten (un-)gerechtfertigter Überwachungspraktiken ausgesetzt sehen, weil die Datenerhebung per se oder die denkbare Datenverwendung den Grad der „höflichen Unaufmerksamkeit“ (Endreß/Rampp 2013: 156f.) überschreitet, den eine Kultur des Taktes im „wechselseitigen Voneinander-Notiz-Nehmen“ (Endreß 2012: 88) etabliert, variiert vielmehr mit den infrage stehenden Daten, Vorstellungen ihrer Verwendung in unterschiedlichen Zusammenhängen und den jeweils zugrundeliegenden Zwecken. Ein Einsatz des Verfahrens etwa zum Zwecke der Zeiterfassung wird regelmäßig abgelehnt, weil diese selbst gegen kontextuelle Bedingungen, das heißt Vorstellungen über die Gestaltung beruflicher Beziehungen, verstößt:

> Günther Konrad (Einwo) ((fällt ins Wort)): „Ne, also, wenn ich, wenn ich, ich hatte auch mal ‘ne Firma, aber würd‘ ich nich‘ machen.“
>
> I: „Würden Sie nich‘ machen. Warum?“

> Günther Konrad: „Weil ich mir die Leute, die ich einstelle, guck‘ ich mir vorher an, und denn beurteile ich das selbst, denn. Is‘ bei ‘ner GmbH oder is‘ das vielleicht anders, aber wenn ich jetzt Einzelunternehmer bin, denn such ich mir meine Leute aus, und dann weiß ich, wenn ich den einstelle, is‘ das auch in Ordnung.“
>
> I: „Das heißt, dann sagen Sie, dem vertraue ich (Günter Konrad: Ja, genau so is‘ es), den muss ich nich‘ kontrollieren.“
>
> Günther Konrad: „Denn die gute Arbeitsleistung krieg ich nur auf ‘ner Vertrauensbasis. Hab‘ ich jedenfalls die Erfahrung gemacht.“

Gehört dieser Vorstellung nach ein vertrauensvolles Verhältnis zu den Bedingungen des Verhältnisses zwischen Arbeitgeber und -nehmer, dann vor allem deshalb, weil dieses als Möglichkeit zur Selbststeuerung gerade Kontrollerfordernisse unnötig macht – ein Zusammenhang, der etwa von Strickland bereits 1958 als Kontrollparadox beschrieben wurde und wonach extensive Kontrolle den Aufbau von Vertrauen verunmöglicht. Der Bedarf an Vertrauen setzt einen beiderseitigen Kontrollverzicht voraus. Ein Einsatz der Technologie zu Zeiterfassungszwecken wird dann mitunter als „indirekter Indikator von Misstrauen“ (Larson 2004: 35) gedeutet: *„Also ich weiß definitiv, dass das Unternehmen mir nich‘ vertraut, sonst würden sie mich nich‘ überwachen.“* (Marius Tapfer, Vid). Wenn sich die kontextuelle Relativität der Bedeutung der Daten also ausdrücklich darin zeigt, dass es für die Befragten darauf ankommt, wem sie zu welchem Zweck ihre Daten anvertrauen, dann deuten sich damit auch kontextuelle „Vertrauensprofile“ (Endreß 2012: 97) an.

3.2.2.2 Vertrauensverhältnisse: Das Ausblenden der unheimlichen Möglichkeiten[59]

Vertrauen ist, wie auch Akzeptanz, sowohl Bestandteil von Umgangssprache, als auch ein theoretischer Begriff und in der Vertrauensforschung variieren abhängig von den jeweils zugrunde gelegten Situationen und Handlungskontexten von Vertrauensverhältnissen die Bestimmungen der Bedingungen vertrauensvoller Erwartungen, mithin des Vertrauens selbst. Dies vermag dann auch die Konkurrenz der zahlreichen Erklärungsansätze begründen, die sich, zum einen, grundverschiedenen Vertrauensverhältnissen und -formen (Hartmann 2011: 33) widmen und, zum anderen, an jeweils spezifischen Punkten der etwa von Möllering (2006) identifizierten Schnittmenge von „reason“, „routine“ und „reflexivity“, der, mitunter in der Forschung zur Vertrauensform verabsolutierten, Vertrauensbedingungen ansetzen. Diese Unterscheidung bezieht sich sowohl auf die Ursachen, als auch auf die Bedingungen der Ver-

[59] Eingang in die nachfolgenden Darstellungen finden in überarbeiteter Form veröffentliche Ausführungen zum Vertrauen, die als Gemeinschaftsarbeit unter dem Titel „Die gesellschaftliche Konstruktion der Sicherheit“ (Krasmann et al. 2014), sowie 2015 unter dem Titel „Gambling with the ‚Gift‘?“ (Kühne 2015) erschienen sind.

trauensgabe: kognitive Abwägungsprozesse, Routinen in der alltäglichen Lebenswelt, welche sich an Regeln und Rollen orientieren, sowie die (reflexiven) Erfahrungen des Vertrauensaufbaus. Wird die Frage nach den Bedingungen von Vertrauensverhältnissen auf Entscheidungssituationen zugespitzt, dann handelt es sich bei diesen, von Möllering (ebd.) unter den Begriff des „reason" gebrachten, Ansätze vor allem um Konzepte, die den Annahmen der Rational-Choice-Theorie folgend, Vertrauen als eine im Wesentlichen bewusste und kalkulatorische Entscheidung unter Risikobedingungen mit dem Ziel der Nutzenmaximierung fassen (vgl. Coleman 1991: 121ff.): Für die dem Moment der Vertrauensgabe zugrundeliegende Unsicherheit über das Handeln des Vertrauensnehmers – kann dieser doch zukünftig das Vertrauen für seine eigenen Zwecken (aus)nutzen und somit enttäuschen – kalkuliert der Vertrauensgeber unter Einbezug des Wetteinsatzes, der Höhe des möglichen Gewinns und der Gewinnchance die Wahrscheinlichkeit, dass sich der Vertrauensgeber als vertrauenswürdig erweist. Erfolgt nun aber ein solch kognitiver Zuschnitt und wird das Vertrauen zudem vor dem Hintergrund möglicher Krisen- oder Desintegrationserscheinungen (vgl. Barber 1983, Coleman 1991) wahrgenommen, dann, so Martin Endreß (2008: 1), weil es sich dabei um einen „Reflex organisationeller Wirklichkeit moderner Gesellschaft" handelt, in der Entscheidungszusammenhänge zunehmend entkoppelt sind und den Bürgern das Wissen fehlt, Gefährdungspotentiale ‚objektiv' einzuschätzen. Eine solcherart reflexive, mithin kalkulatorische Zuwendung zum Vertrauen deutet auf eine Notwendigkeit zu vertrauen hin, da es das grundlegende Zeit- und damit verbundene Informationsproblem bewältigt (vgl. Preisendörfer 1995: 264). Die Wahrnehmung der Fingerabdrucktechnologie als ambivalent (vgl. Kapitel 3.1.2) – aufgrund der kontingenten Schadensmöglichkeiten, die also weder in ihrer Fülle abseh-, noch individuell abwendbar erscheinen –, führt die Frage des Vertrauens insofern bereits definitorisch in jene nach der Akzeptanz ein.

Statt für die Bedeutung des Vertrauens im Kontext von Akzeptanz jedoch eine kalkulatorische Konzeption anzunehmen, wird Vertrauen in einem allgemeinen Sinne zuallererst als ein Modus verstanden, Ungewissheit aufzuheben (vgl. Möllering 2006). Es etabliert sich dort, wo kein umfassendes Wissen oder explizites Wissen vorhanden ist bzw. sein kann. In Georg Simmels (1992: 393) Worten ist Vertrauen

> „ein mittlerer Zustand zwischen Wissen und Nichtwissen um den Menschen. Der völlig Wissende braucht nicht zu vertrauen, der völlig Nichtwissende kann vernünftigerweise nicht einmal vertrauen."

Vor allem Niklas Luhmann (2000) hat diese Funktionalität eines solchen Grundvertrauens betont, indem er Vertrauen als Handlungsermöglichung unter Bedingungen von Komplexität

und Kontingenz, insofern als Entscheidung unter dem Eindruck multipler Möglichkeiten verhandelt. So nimmt, wer vertraut „Zukunft vorweg“ (ebd.: 9) und gewinnt in der Gegenwart Sicherheit (ebd.: 13), indem Vertrauen in Kontinuitätserwartungen [übergeht], die ohne Reflexion wie feste Gleitschienen dem täglichen Erleben zugrunde gelegt werden.“ (ebd.: 29) Vertrauen ermöglicht, trotz einer an sich kontingenten Zukunft, ein Handeln, das sich der eigenen Erwartungen versichern kann und so bewirkt, diesen zu vertrauen (ebd.: 1ff.). Ein solches Welt-, Ur- oder Grundvertrauen, etwa die implizite Erwartung, dass Gebäude nicht ein- bzw. Fahrstühle nicht abstürzen oder Passanten einander nicht unvermittelt angreifen, grenzt Luhmann (2001) in einem späteren Aufsatz[60] als Zuversicht vom Vertrauen ab, da es nicht als Entscheidungsnotstand unter Risikobedingungen gefasst werden kann. Für Martin Hartmann (2011: 114) hingegen ist das scheinbar „gedankenlose“ alltägliche Vertrauen, vielmehr „eine soziale und kulturelle Errungenschaft, die sich auf individueller Ebene als eine habitualisierte Einstellung einer weitgehend reflexionsfreien vertrauensvollen Zuversicht auslegen lässt.“[61]

Als Modus eines „Verhältnisses“ (ebd.: 17), ob nun zu Personen oder Institutionen, bedeutet Vertrauen einen bewussten Verzicht auf vollständiges Wissen (Luhmann 2000) als Mittel der Kontrolle. Damit ist Vertrauen aber auch riskant, denn das Moment der Vertrauensgabe beinhaltet auch immer eine Verletzungsoffenheit, die in der Anerkennung der Freiheit der anderen – auch immer anders handeln zu können –, liegt (vgl. Baier 2001): Vertraut man diesen, dann räumt man ihnen die Gelegenheit der Verletzung ein. Guido Möllering (2006: 191) hat den Modus der Verarbeitung dieses Moments der Verletzungsoffenheit im Vertrauen als einen „leap of faith“– einen Vorschuss und gleichsam Vertrauenssprung ins Ungewisse – bezeichnet. Er erfasst damit die Ambivalenz des Vertrauens, wenn die Freiheit des Anderen und damit die mitunter schweren Konsequenzen, die diese potentiell mit sich bringt, anerkannt und im gleichen Zuge aufgehoben werden, weil man sich zuversichtlich zeigt, dass dieser die Verletzungsgelegenheit nicht nutzen wird (Baier 2001: 43). Anders als in der Luhmannschen Konzeption wirkt das Vertrauen auf diese Weise dann nicht als Reduktion von Unsicherheit – werden doch Unsicherheiten und Risiken nicht im Sinne einer „erwerbbaren Versicherungsgarantie“ (Endreß (2001: 183) verringert. Vielmehr handelt es sich dabei um ein Aufheben

[60] Der 1988 veröffentlichte Aufsatz „Familiarity, Confindence and Trust: Problems and Alternatives“ erschien 2001 erstmals in einer deutschen Fassung in dem von Martin Hartmann und Claus Offe herausgegebenen Sammelband „Vertrauen. Die Grundlage des sozialen Zusammenhalts“.

[61] Für Martin Endreß, der den Zuschnitt der Luhmannschen Konzeption ebenfalls aus dem Korsett der modernisierungstheoretischen Differenzierung von Gefahr und Risiko befreien möchte, handelt es sich um zwei Modi des Vertrauens, die sich zwischen habitueller Einstellung und einer vorreflexiven Haltung des „Zur-Welt-Sein“ bewegen (2002, 2012). Unter dieser Perspektive wäre dann auch mit Hartmann (2011: 114) die Sicherheit, mit der wir uns in der Welt bewegen nicht natürlich gegeben, sondern das Resultat einer „zivilen Praxis […], in deren Rahmen bestimmte Gefahren erfolgreich gebannt oder überwunden werden konnten“.

bzw. Suspendieren von Unsicherheit, das heißt diese wird gleichsam „negiert und bewahrt“ (Möllering 2007: 73). Mit Bezug auf Simmel veranschaulicht Möllering (2006: 11) das Vertrauen als ein so tun als ob („as if“) keine Unsicherheiten vorhanden wären. Mit Vertrauen wird folglich eine positive Erwartung verbunden, „dass andere durch ihr Handeln oder Unterlassen zum Wohlergehen eines einzelnen oder einer Gruppe beitragen, jedenfalls von schädigenden Handlungen absehen.“ (Offe 2001: 249)

Vor diesem Hintergrund lässt sich in den nachfolgenden Ausführungen zeigen, dass ein so verstandenes Vertrauen für eine Reihe von Befragten die Voraussetzung dafür bildet, dass die riskanten Möglichkeiten der Datenverwendung ausblendet werden und das Verfahren im eigenen Anwendungssetting in dieser Hinsicht unproblematisch wird. Vertrauen als Akzeptanzbedingung lässt sich über die Anwendungssettings hinweg gleichwohl entlang unterschiedlich ausgeprägter Reflexivitätsgrade verfolgen, also von eher präreflexiven (Hartmann 2011) bzw. „fungierenden“ (Endreß 2001, 2002) und insofern eher unbewussten Vertrauensmodi, die sich vor allem im Hinblick auf Bekanntheit konstituieren, bis hin zu bewussten Entscheidungen, die gleichwohl nicht immer abwägender Natur im Sinne eines Gegenüberstellens von Vor- und Nachteilen sein müssen. Das heißt auch, dass für die nachfolgende Betrachtung nicht von vornherein die Bestimmungen vertrauensvoller Erwartungen zugrunde gelegt werden. Nun ließe sich einwenden, dass es zur „Grammatik des Vertrauens“ (Hartmann 2011: 39) gehören könnte, dass die sinnvolle Anwendung des Begriffs das Unbewusste des Vertrauens voraussetzt, sich die Befragten eben „nicht explizit darüber im Klaren sind, dass sie […] vertrauen“ (ebd.). So ist die Explikation des Vertrauens, etwa Endreß (2001: 203) zufolge, bereits „eine Problemanzeige und überführt Vertrauen aus seinem fungierenden Modus in den Bezugsrahmen von Wahl und Entscheidung.“ Der Annahme folgend, dass Vertrauen gewiss das reflexive Abwägen verkürzt, ist es allerdings dennoch möglich, bei dem von den Befragten explizierten Vertrauen eine gewisse Vorgängigkeit zu unterstellen, weil in den, in den Interviews hervorgebrachten, Vertrauensexplikationen die Bezüge des Handelns geordnet werden. Damit kommen, zum einen, ex post die vormals impliziten Gründe der Vertrauensgewähr zum Ausdruck, die das Nutzungshandeln als Vertrauenssprung rechtfertigten. Vertrauen in dieser Weise und als ein Ergebnis der Analyse zu thematisieren, folgt dann im Grunde der von Möllering (2006: 131) formulierten Strategie, sich dem Phänomen des Vertrauens anzunähern:

> „It requires a process perspective, obtaining a rich (typically qualitative) picture of actual trust experiences, understanding the embeddedness of the relationships under investigation and taking into accout the reflexivity not only in trust development as such but also in the research interaction. The general orientation should get away from

> measuring predefined variables and get closer to the respondents' idiosyncratic experiences and interpretations."

Mit den reflexiv gewordenen Beweggründen, die im Vertrauen münde(te)n, – Erzählungen über den Charakter sozialer Beziehungen, die Wahrnehmung von Situationen und Umgangsformen oder auch spezifische Zuschreibungen zur fingerabdrucknehmenden Instanz – lässt sich dann, zum anderen, der Eigenwert des Vertrauens, als eine Bedingung von Akzeptanz eruieren.

3.2.2.2.1 Vorgängiges Vertrauen durch Vertrautheit

Vertrauen ist, obgleich auf die Zukunft gerichtet, vergangenheitsorientiert. In seinem Bezug auf eine vertraute Welt, die, wie Luhmann (2000: 23, vgl. 9ff.) es ausdrückt, als „Hintergrundsicherung" die Erwartungen an die Zukunft ermöglicht, basiert es auf der zeitlichen, räumlichen sowie sozialen Generalisierung von Erfahrung. Dies verweist auf *Vertrautheit* als seine Voraussetzung (Luhmann 2000: 23). Dabei handelt es sich um ein sich in Bezug-setzen zur Welt, „das Typizität" (ebd.: 23) sozial konstituiert. Unter Bezug auf Helmut Plessner und Alfred Schütz erweitert Martin Endreß (2001) diesen Blick auf den Prozess der Typisierung für die Frage des Vertrauens, indem er das Konzept der Vertrautheit als das fraglos Hingenommene konzipiert. Danach handelt es sich bei der Vertrautheit nicht nur um eine Beschreibung für den Zustand einer Beziehung oder der Geläufig- bzw. Verbindlichkeit eines Sachverhalts (ebd.: 167), sondern der Begriff bezieht sich auf ein haltungsspezifisches Vorverständnis zur Welt (ebd.: 175). Vertrautheit wird interaktionistisch durch die Generalisierung von Erfahrung gewonnen, das heißt sie unterliegt einem dauernden Prozess der Transformation von Unvertrautem in Vertrautes (ebd.: 166ff.). Es ist dieses Spannungsverhältnis zwischen lebensweltlich Vertrautem und Unvertrautem, das zu Normalisierungspraktiken im Alltag in Form von Routinen und Typisierungen führt (ebd.: 180 mit Bezug auf Plessner und Schütz), die gleichsam ihren Ursprung in wechselseitigen Verhältnissen haben (ebd.: 185):

> „Vertrauen zu können wie Vertrauen zu haben basiert auf vergangenen Erfahrungen, auf spezifischen Wissensbeständen, die (zumindest) einen Menschen als vertrauenswürdig erwiesen, eine Technik als funktionierend bzw. erprobt oder bewährt präsentiert oder eine Experten als kompetent ausgewiesen haben" (ebd.: 175).

Vertrautheit bezieht sich auf selbstverständliche Routinen, die von einer bewussten Reflexion von Handlungen und Entscheidungen entlasten, indem „man unterstellt, dass sich das Bekannte fortsetzen wird – die Zukunft wird sich schon nicht völlig anders gestalten als die Vergangenheit" (Osterloh/Weibel 2006: 42). Barbara Misztal (2001: 314) unterscheidet für das

Normalitätsempfinden eine faktische Dimension – die Regelmäßigkeit von Ereignissen und Verhalten – von einer normativen Komponente der Normalität, die sich in der Klassifizierung einer Handlung als normkonform ausdrückt. Vor diesem Hintergrund verweisen die Befunde aus den Befragungen mit Antragstellern im Einwohnermeldeamt für die Akzeptanz der Fingerabdrucktechnologie auf die Bedingungen einer vertrauten Normalität der Datenpreisgabe. Diese schlägt sich exemplarisch darin nieder, dass für manche Antragsteller keine Irritationen darüber entstehen, dass ein bislang nicht bekanntes Datum neuerdings erfasst wird und in Anerkennung der legitimen Sicherheitszwecke mit dem Fingerabdruck dann auch die Papiere *„korrekt“* (Hans-Peter Janßen, Einwo) gewusst werden. Vertraute Normalität ist dann auch die Basis für die Preisgabe der Fingerabdrücke zu Sicherheitszwecken, trotz fehlender persönlicher Relevanz. Mit dieser Annahme von der Normalität einer Situation wird vertrauensvolles Handeln ermöglicht, es reduziert ihre Komplexität und gestattet es, dem Gegenüber vertrauensvoll zu begegnen.

Vertrautheit bezieht sich aber nicht nur auf gewohnte Handlungsabläufe und Situationen, sondern auch auf Personen, die zum Beispiel durch einen längeren zeitlichen Kontakt sehr gut bekannt sind (vgl. Endreß 2001: 167). Wenn also die Befragten im Supermarkt oder auch in der Zahnarztpraxis die Fingerabdruckabgabe als unproblematisch bewerten, dann vor allem deshalb, weil sie mit den Fingerabdrucknehmern eine hohe Verlässlichkeit verbinden. Die Motive ihrer Nutzung reflektierend, beziehen sich die Befragten in den Interviews, häufig für sie selbst überraschend, dann auf eher implizite Vertrauensgründe, die ihren Entscheidungen zugrunde lagen, wie etwa nachfolgend die 56-jährige Elisabeth Müller (Sm):

> „Also ich mein, ich würd jetzt nicht in jedem Geschäft so was hinterlegen, aber, wie gesagt, dass ‚Boll‘ [Name des Supermarkt-Inhabers], der ist ja schon seit Jahrzehnten da, und da wir, ich weiß nicht, Sie kennen sich in [Name der Stadt] nicht aus, (I: Leider nein) wir wohnen in [Name des Stadtteils], das is‘n Seitenteil, das kein eigenes Geschäft hat, und so ist also [Name des Stadtteils] praktisch der erste Anlaufpunkt, und wie gesagt, seit es das ‚Boll‘ gibt, kaufen wir dort ein, insofern, also, steht zumindest von meiner Seite aus, ja so‘n gewisses Grundvertrauen, sag ich jetzt mal, ne? Die Familie ist auch schon lange ansässig, die hatte vorher schon‘ n kleines Geschäft, Stückchen weiter unten, und ich bin geborene [Einwohnerin des Stadtteils] auch, also. Ist schon auch ‘ne Frage ob ich, also ich würd‘ das jetzt nicht in jedem Geschäft machen.“

Frau Müller spricht hier in Bezug auf ihre Entscheidung, die Fingerabdrücke zum Zweck der Bezahlung im Supermarkt zu nutzen, über den Aufbau einer, mittlerweile etablierten, Vertrauenshaltung gegenüber dem Supermarktinhaber und verweist zugleich auf die Bedingungen, die diese hervorgebracht haben: Es sind ein Gefühl gemeinsamer Zugehörigkeit durch Nachbarschaft (im Stadtteil) und eine lokale Identität, die sich aufgrund der mit der Familie

des Supermarkts geteilten Geschichte herstellt, welche für Frau Müller ein Gefühl von Sicherheit erzeugen, mit der potentielle Risiken der Datenpreisgabe von vornherein ausgeblendet bleiben. Diese spezifische Erfahrung von Nähe führt dazu, dass in diesem Fall der Treunehmer, anders als große Discounter-Ketten, die gleichwohl ebenfalls in ihrer lokalen Nähe vorhanden sind, ein ‚Gesicht' besitzt, an das sie ihre persönlichen Nutzungsbedingungen knüpft: *„Zum Beispiel zu so 'nem großen Unternehmen wie [Name einer bekannten Discounterkette] oder so, mm, nee. Nee. Da würd' ich mich jetzt nicht dazu verleiten lassen."* (Elisabeth Müller, Sm). Die Durchführung eines potentiell riskanten Handelns, wie es sich mit dem *„sich verleiten lassen"* andeutet, bedarf folglich spezifischer Bedingungen, die sich für Frau Müller erst aus dem Gefühl von Verbundenheit zum Supermarktbesitzer ergeben.

Bei der Entscheidung zur Nutzung des Verfahrens wird aber nicht nur im Kontext von Freiwilligkeit eine spezifische Nähe zum Fingerabdrucknehmer, welche ein Gefühl der Vertrauenswürdigkeit vermittelt, als weitere Bedingung für die Nutzung des Verfahrens relevant. Auch für Kathleen Häuser (Arzt), eine Angestellte der Arztpraxis, entproblematisiert sich das Fingerabdruckverfahren durch eine jahrelange Bekanntschaft mit dem leitenden Arzt, der die Fingerabdruckdaten für das Zeiterfassungssystem verwaltet:

> I ((fällt ins Wort)): „Würden Sie jetzt zum Beispiel bei so 'ner Automatenvideothek (Kathleen Häuser: Nee), das in so 'nem Rahmen nich' verwenden?"
>
> Kathleen Häuser ((fällt ins Wort)): „Nee, das würd' ich nich' machen. Nee. (I: Okay) Da hätt' ich 'n, da hätt' ich 'n komisches, da hätt' ich wirklich 'n komisches Gefühl dabei, da denn irgendwo meinen Fingerabdruck abzugeben und dann (I: Ja) weiß man nich', wer dahinter sitzt, was da passiert mit, wer da noch alles drauf Zugriff hat, das, nee. Das würd' ich nich' machen."
>
> I: „Also einfach, weil Ihnen nich' klar wäre, was dann mit den"
>
> Kathleen Häuser: „Genau, das is' so undurchsichtig (I: damit geschieht). Ja. Es geht durch viele Hände dann auch meistens, also is' ja denn nich' so wie hier, dass es dann mein Chef is', den ich schon seit vielen Jahren kenne, sondern das, ja, das würd' ich nich' machen."
>
> I: „Is' das so 'ne Frage von Vertrauen dann in dem Moment, sodass Sie dann"
>
> Kathleen Häuser ((fällt ins Wort)): „Definitiv ja. Ich, wenn ich ihn jetzt, was weiß ich, erst 'n halbes Jahr kennen würde, dann hätt' ich wahrscheinlich auch 'n anderes Gefühl gehabt (I: Ja), ‚Jetzt geben Sie mal hier Ihren Fingerabdruck ab, das is' hier für unsere Zeiterfassung.' (I: Ja) Aber das, doch das hat schon was mit Vertrauen zu tun. (I: Ja) Ja."

Für Kathleen schafft sowohl die faktische Nähe – sie begegnet ihrem Arbeitsgeber regelmäßig –, als auch eine so über die Jahre etablierte Vertrautheit mit ihrem Arbeitgeber ein Gefühl von Transparenz im Hinblick auf die mutmaßliche Datenverwendung. Sie hat auf diese Weise einen Eindruck von seinem Handeln gewonnen, das nicht nur das eigentlich *„komische"* Fin-

gerabdruckverfahren normalisiert, sondern sie auch einen Missbrauch der Daten ausschließen lässt.

Allerdings setzt ein solches in die Fingerabdrucknehmer investiertes Vertrauen nicht zwangsläufig regelmäßige direkte Interaktionen mit diesen voraus. Vertrautheit wird etwa im Supermarktsetting auch indirekt über den regelmäßigen Besuch des Supermarktes, mithin ‚Herrn Bolls Supermarkt', vermittelt: das Geschäft ‚steht für' den Betreiber, denn regelmäßig sprechen die Befragten nicht von der Supermarktkette, zu der dieser gehört, sondern verwenden den Eigentümer-Namen. Bezugspunkt für vertrauensvolle Erwartungen ist in diesem Setting eine im zeitlichen Verlauf gewachsene und mutmaßlich erfüllte Erfahrung bezüglich einer sozialen Reputation (zur Entwicklung von Reputation vgl. Eisenegger 2015: 38) des Inhabers. Diese beschert ihm einen Ruf von Vertrauenswürdigkeit, der ihm mithin vorausseilt, worauf zum Beispiel Herr Bauman (Sm) im Interview nachdrücklich hinweist:

> „Ja, ich, also, bitt'schön, das, das, das, das Vertrauen kommt durch die, durch die Firma, nicht? Also, wenn Boll was macht, dann, dann ist das ordentlich, nicht? Also, davon gehe ich immer aus, und, da wir seit Jahren da Kunden sind."

Aufgrund dieses Vertrauens in die offenbare Rechtschaffenheit des Besitzers – dass eben auch ein eher mit Unsicherheiten verknüpftes Verfahren eben *„ordentlich"* installiert wird –, vertraut Herr Bauman dem Inhaber nicht nur die Fingerabdruckdaten an. Bei der Registrierung lässt er zudem seine Telefonnummer aufnehmen, was eigentlich ein Risiko ist, da ihm unerwünschte Anrufe, wie er bei der Anmeldung berichtet, höchst unangenehm sind. Aber auch hier sei dies eine *„Sache, des Vertrauens, die ich zu der Firma Boll habe"*, also eine Erwartung, dass der Umgang im Supermarkt orientiert ist am Wohlbefinden der Kunden (zur „Benevolenzerwartung" vgl. Osterloh/Weibel 2006: 59ff.).

Vertrauen als Akzeptanzbedingung etabliert sich im Supermarktsetting folglich primär aufgrund lokaler Bekanntheit, die es ermöglicht Informationen, die in der Vergangenheit gewonnen wurden, im Hinblick auf das zukünftige Verhalten des Supermarktinhabers zu „überziehen" (Luhmann 2000: 23) und so auch einen Umgang mit den eigenen Daten zu erwarten, der keinen subjektiven Nachteil mit sich bringt. Unter diesen Voraussetzungen kann man dann auch unbedenklich ein Angebot des bekannten Supermarktbesitzers annehmen. Theoretische Nachteile werden in diesem Setting praktisch nicht relevant. Für diese Vertrauenshaltung bedarf es, wie die Interviews zeigen, offenbar weder spezifischer Zurechnungen zur Glaubwürdigkeit im Hinblick auf die Verwendung der biometrischen Daten, noch Wissen um die konkreten Sicherheitsvorkehrungen. Die Interviewten spezifizieren nur selten ihre Erwartungen etwa zur Datensicherheit oder konkreten Datenschutzvorkehrungen, die mutmaßlich durch

den Betreiber des Supermarktes vorgenommen werden. In der Regel bleibt der *„sorgfältige“* Datenumgang (Erika Hundt, Sm) im Zustand der Vertrautheit eher eine latente, im spezifischen Verhältnis „unterstellte gesicherte Orientierung“ (Endreß 2001: 167), die sich in der Erwartung an die Zuverlässigkeit des Betreibers gründet und insofern weniger eine etwa technische Kompetenz, als vielmehr eine spezifische Integrität des Inhabers stillschweigend voraussetzt. Lediglich Rolf Burger (Sm) leitet aus der Lokalität des Verwendungskontextes Vorstellungen über das verwendete System der Datenverwaltung ab. Analog zu der Begrenztheit des Settings – das Fingerabdruckverfahren ist nur in diesem Supermarkt verfügbar – geht er von einer lokalen Datenspeicherung aus, aufgrund derer sich für ihn auch die theoretischen Möglichkeiten des Zugriffs auf die Daten begrenzen:

> „zumal ich hier halt meinem, meinem Herrn Boll halbwegs vertraue, dass das, und [Name des Supermarktes] in dem System drinne ist, in dem sich auch wenig Leute bewegen, die irgendwie was haben möchten. Ich mein‘, Sony arbeitet global, er arbeitet lokal.“

Dabei ist es für Herrn Burger gerade die Lokalität, und das durch sie generierte Wissen, aufgrund derer theoretische Nachteile ausgeschlossen werden und dies in einem, in doppelter Hinsicht, physisch begrenztem Raum. Weil sich die Befragten im Setting Supermarkt auch als Teil einer überschaubaren Gemeinschaft begreifen, in der man sich zumindest hin und wieder begegnet, kreiert diese Nähe für Herrn Bauman dann auch ihre eigenen Sicherheitsmechanismen, wenn er im Interview darauf hinweist, dass *„wenn bei Boll was passiert, dann bleibt das schön in [Name des Beobachtungsortes], nicht?“* Damit verweist Herr Bauman nicht nur auf eine spezifische Sanktionsmöglichkeit missbrauchten Vertrauens, die Niklas Luhmann (2000: 46) als das „Gesetz des Wiedersehens“ beschrieben hat, sondern auch auf einen instrumentellen Wert seines investierten Vertrauens, der sich aus der Reziprozität von Vertrauensverhältnissen – die eben keine Abhängigkeitsverhältnisse sind (Endreß 2001: 170) – ergibt. Auf diese Weise erscheint die potentielle Gelegenheit zur Verletzung durch den Supermarktinhaber begrenzt, weil Herr Bauman davon ausgeht, dass etwa ein missbräuchlicher Umgang mit den Fingerabdruckdaten das Eigeninteresse des Supermarktinhabers an einem wohlwollenden, mithin vertrauenswürdigen Handeln verletzte. Dieser riskierte gegebenenfalls nicht nur den Abbruch einer etablierten Geschäftsbeziehung, sondern dies käme einer Blamage gleich und würde seiner Reputation schaden, könnte er dann doch den Bürgern des Ortes nicht mehr in die Augen schauen.

Diese verpflichtende Wechselseitigkeit als impliziter Kontrollmodus wird auch von im schulischen Setting befragten Eltern ins Feld geführt, die potentielle Unabwägbarkeiten des Verfah-

rens durch Erwartungen eines Eigeninteresses der Stadt – als einführender Instanz des Verfahrens – an verbindlichem Handeln relativieren:

> I: „Ja. Was genau und wo das [die Fingerabdruckdaten] gespeichert ist? Wissen Sie das?“
>
> Christa Jürgens (Schul1): „Nee, des weiß ich nich‘ ganz genau, aber ich meine, so oder so müsst, also, wenn Banken gehackt werden können, dann kann man das auch hacken. Dann ist es mir eigentlich grad egal, wo des gespeichert is‘. Dann vertrau‘ ich darauf, dass, es ist ja auch von der Stadt begleitet dieses System. Auch von der Stadt eingeführt, insofern kann ich davon ausgehen, dass es ordentlich, handwerklich ordentlich gemacht ist […] Also, wenn ich, wenn ich schon Daten von mir preisgebe, dann, doch wirklich gezielt und nich‘ in so ‘nem. Also da, da, da weiß ich, dass die Stadt das aller größte Interesse daran hat, dass sie nicht in die Schlagzeilen gerät, dass das sauber und ordentlich abläuft.“

Wie Herr Bauman formuliert Frau Jürgens ein gegenseitiges Interesse an Datensicherheit als vorausgesetzte Verbindlichkeit in einem spezifischen Verhältnis von Fingerabdruckgeber und -nehmer. Das ‚Interesse‘ der Stadt als „manifester Aspekt der Sanktionsmöglichkeiten“ (vgl. Luhmann 2000: 46) ermöglicht nicht nur im Vertrauen die Ungewissheiten der riskanten Datenverwendung aufzuheben. Zugleich strukturiert es die Zuschreibung von Verantwortlichkeiten, die ursprünglich daraus resultieren, die Daten der eigenen Kinder preisgegeben zu haben.

3.2.2.2.2 Bestätigtes Vertrauen durch Authentizität und soziale Billigung

Vertrautheit ist auch im Videothekenkontext von Bedeutung, wenn hier, wie in Kapitel 3.1.1.1 bereits ausgeführt, die institutionellen Regeln der Verifikation von Identität als gegeben anerkannt werden und eine in diesem Sinne „eingelebte Praxis“ (Endreß 2001: 169) motivierend wirkt. Dass auch hier Vertrauensvorschüsse, als einem spezifischen Personenvertrauen, gegeben werden, lässt sich allerdings, anders als im Supermarkt, zunächst nicht durch eine vergleichbare Bekanntheit und Erfahrungen von Verlässlichkeit erklären. Die Videothekennutzer können bei der Anmeldung nicht auf zeitlich länger andauernde Erfahrungen zurückgreifen, da die Speicherung der Fingerabdrücke Voraussetzung der Nutzung des gesamten Settings ist. Stattdessen müssen sich die Nutzer bereits während des kurzen Registrierungsprozesses mit dem Inhaber vertraut machen. Spielt auch hier, wenngleich in nur wenigen Fällen, ein ausdrückliches Vertrauen eine Rolle, dann ziehen diese Nutzer ihre vertrauensvollen Erwartungen vor allem aus dem persönlichen Eindruck, den sie vom Videothekenbesitzer gewonnen haben. Von Relevanz für Beurteilungen seiner Verlässlichkeit und Vertrauenswürdigkeit erweist sich hier also eine Vertrauensvoraussetzung, die James Henslin (1968: 140) in Anlehnung an Goffmans „Impression management“ identifiziert. Vertrauen entsteht danach

aus Signalen von Vertrauenswürdigkeit, die aus der Wahrnehmung der Selbstpräsentation des Gegenübers abgeleitet werden, also dann, wenn „an actor has offered a definition of himself and the audience is willing to interact with the actor on the basis of that." (ebd.) Ist diese Präsentation bei Henslin primär eine taktische Performance, dann illustriert diese sich auch in der nachfolgenden Passage aus dem Interview mit dem Betreiber der Videothek, in der dieser beschreibt, wie er regelmäßig im Umgang mit seinen Kunden gesehen werden möchte:

> „Und, aber ich hab' immer gesagt zu den Leuten, ich hab' hier [im Stadtteil] 'n guten Ruf, man kann sich hier gerne über mich erkundigen, ich hab' hier noch nich' eine Adresse rausgegeben und diese Fingerprints, hab ich dann gesagt, kann ich eh' nich' rausgeben, weil ich gar nich' weiß, wo die sind." (Andre Behringer, Vid)

Setzt der Inhaber auf Reputation, die den möglichen Nutzerschaden ausschließen soll, spielt dies für die Kunden im Moment der Registrierung, wie beschrieben, schon aufgrund des Zeitproblems entsprechende Informationen einzuholen und ihres in der Regel pragmatischen Interesses eine fußläufig zu erreichende Videothek zu nutzen, eine eher untergeordnete Rolle. Von Bedeutung erweist sich dann vielmehr die Authentizität seiner Selbstdarstellung, mit der er Desinteresse als auch technisches Unvermögen in Bezug auf die Datenweitergabe kommuniziert. So wird er etwa als *„nett, freundlich, serviceorientiert"* (Corinna Meier, Vid) beschrieben und habe in der Registrierungssituation *„nichts Dubioses"* gefragt, das explizite Zweifel hervorgerufen habe (Max Schaf, Vid). So räsoniert Max (Vid) dann auch: *„irgendwo vertraut man dem."*

Zwei Gründe für die Rechtfertigung eines solch implizit erteilten Vertrauensvorschuss lassen sich identifizieren. Zum einen wird das regelmäßige Nicht-Funktionieren der Maschinerie Videothek bei einem gleichermaßen hohen Vertrauen in die Technik, wie sie bereits als unhinterfragte Funktionsunterstellung thematisiert wurde (vgl. Kapitel 3.1.3), zur Bestätigung für die Annahme, dass kein Nachteil durch den Betreiber zu erwarten ist. Bedeutsam wird in diesem Setting gerade das technische Nicht-Funktionieren, denn die Mechanisierung sozialen Handelns gerät, wie in Kapitel 3.2.1.2.2 skizziert, im automatisierten Kontext Videothek in unterschiedlicher Weise an ihre Grenzen – weil etwa mal die Zugangskarte nicht funktioniert, der Fingerabdruck nicht eingelesen oder auch DVDs nicht erfolgreich am Automaten zurückverbucht werden können. Dass der Betreiber verlässlich an zwei Tagen vor Ort und bei Problemen per Mail oder Telefon erreichbar ist und von den Nutzern als jemand erfahren wird, der auch unkonventionell bei Problemen Abhilfe schafft, bestätigt dann den situationsbasierten Eindruck, dass es sich bei ihm um eine zuverlässige Person handelt, der man im Hinblick auf ihre Aussagen trauen kann und das Personenvertrauen verstetigt sich. Auch bei anfänglichen Zweifeln an der Wahrhaftigkeit seiner Aussagen, die manchen Befragten zunächst ein Gefühl

latenter Unglaubwürdigkeit vermittelten – das Vertrauen insofern zunächst nur unter Vorbehalt gewährt wurde –, sind es dann die *„kleinen Unzulänglichkeiten, in Anführungsstrichen"*, die den Vorschuss des Vertrauens rechtfertigen, weil sie, wie ein Nutzer, der als einziger erklärt, aufgrund seiner *„Bedenken"* Datenschutzfragen während der Registrierung an den Betreiber gerichtet zu haben, *„letzten Endes sozusagen eine Bestätigung der Angaben [sind,] die er mir gegenüber gemacht hat"* waren (Karsten Gald, Vid). In diesem Zusammenhang ist es dann auch die Überschaubarkeit – der kleine Inhaber-geführte Laden *„an der Ecke"* (ebd.), mit dessen einzigem Mitarbeiter man zumindest ab und an in Kontakt kommt, das, vergleichbar mit den Einschätzungen im Supermarkt, zudem ein Gefühl von Authentizität erzeugt.

Zweitens zeigt sich das Vertrauen für Befragte rückblickend als sozial vermittelt und weniger an das konkrete Verhalten des Betreibers geknüpft, wie der Nutzer Max Schaf (Vid) in der nachfolgenden Passage ausführt:

> „Ja, ich weiß es nich'. Ich hab' mir da eben, wie gesagt, keine großen Gedanken gemacht und ich wüsste nich', was er damit irgendwie anfangen sollte. Klar, irgendwo vertraut man dem, glaub ich auch, also irgendwie hatt' ich dann irgendwie das Gefühl, das is' 'ne Videothek, da sind auch andere Leute angemeldet, sag ich mal so, ich hab da schon Leute reingehen seh'n, ich bin da nich' der Einzige und es scheint zu funktionieren und das is' immer so'n Aspekt, dass man glaub ich, wenn man tatsächlich sowas sieht, mit so 'nem Laden davor oder so, dass das tatsächlich 'n Laden is', auch wenn der noch so komisch is' und man sieht da auch Leute da rein und raus geh'n und die schein' das auch zu nutzen und dann denkt man: Ok."

Das hier zum Ausdruck gebrachte Vertrauen generiert sich also nicht nur durch Eigenerfahrungen, sondern ist, in Anlehnung an Schütz (1972: 98), „sozial abgeleitet", das heißt es findet seine Bestätigung auch durch die beobachteten Erfahrungen anderer. Über die sich in deren Nutzung ausdrückender sozialer Billigung (vgl. ebd.: 100) der Fingerabdruckgabe im Setting Videothek bestätigt sich das gewährte Vertrauen. Es wird dann auch zum Indiz einer unproblematischen, zumindest stillschweigenden Hinnahme Vieler, an dem dann mitunter auch ein gewisses Unbehagen an dem Verfahren in der Schule gemessen wird, wie in den nachfolgenden Passagen aus dem Interview mit einer Mutter, deren Kinder das Gymnasium besuchen, deutlich wird:

> I: „Mh, ja. Sie haben grad gesagt, so Datenschutzbedenken waren nich' unbedingt Ihre? Haben Sie sich irgendwie vorher informiert, wo das abgespeichert wird oder welche Daten?"
>
> Monika Reckling ((fällt ins Wort)): „Ja, ich hab' ihm, glaub ich, gesagt, da, also ich bin da jetzt nich' der Freak, der da jetzt, sich hinter jeden, ich bin, ich seh' immer noch das Positive im Menschen, ja, nich' hinter jedem schon wieder 1.000 Fallen da sieht, also ich, die haben ja gesagt, was weiß ich, ich hab das dann jetzt einfach mal geglaubt, ja."
>
> I: „Ja, ok." ((lacht)).

> Monika Reckling: „Mag naiv gewesen sein, aber da wir jetzt keine schlechten Erfahrungen gemacht haben, hab‘ ich auch keinen Grund, da irgendwie dran zu zweifeln.“
>
> […]
>
> Monika Reckling: „Ich hab‘ ja heut‘ morgen [im Anschluss an die Informationsveranstaltung] erstmal gefragt: ‚Sagt mal, macht Ihr eigentlich Fingerprint?‘ Weil ich das, weil ich wusste, Sie sind da und dass die dann auch noch andere Meinungen hören wollten. Aber ich weiß das gar nich‘, wer Fingerprint macht. Aber es kamen ja prompt drei Neue hinein: ‚Aber ich möchte anmelden‘, ja, also ((lacht)), ne. So verrufen scheint das System ja dann nich‘ zu sein.“

Auffällig an dieser Passage ist ein Rechtfertigungsdruck, den die Befragte zu erleben scheint. Augenscheinlich ist hier ein vorgängiges Vertrauen durch die Anwesenheit von zwei Sozialwissenschaftlern, die dem Verfahren durch eine offizielle Studie Problematizität verleihen, zumindest für einige Momente, fraglich geworden. Frau Reckling spricht im Interview dann auch entschuldigend von einer *„naiven“* Haltung, die sie in schnellem Anschluss mit einer generellen Vertrauensneigung gegenüber dem Verfahren in der Schule rechtfertigt. Dass sie zudem explizit eine soziale Billigung einholt, dient dann der Selbstvergewisserung ihrer eigenen Erwartungen, die durch eine relevante Bezugsgruppe – hier: namentlich bekannte Eltern – erfahren wird, welche über ihre Nutzungsbekundungen einen latenten Zweifel an der Glaubwürdigkeit der vom Schulleiter gemachten Aussagen aufhebt, und wie sie, das *„einfach mal glauben“*. Auf diese Weise treten, mutmaßlich durch das Interview induzierte, Datenschutzschutzbedenken für Frau Reckling erneut in den Hintergrund.

3.2.2.2.3 Ausdrücklich vergebenes Vertrauen: Der Fingerabdruck als Gabe

Für Nutzer des Supermarkts und ebenso für einige Befragte in der Videothek generiert sich die Verlässlichkeit ihrer eigenen Wahrnehmung, dass die Nutzung der Technologie keine negativen Folgen zeitigt, vor allem aus mehr oder weniger direkten Interaktionen mit dem jeweiligen Anbieter. In diesem Zusammenhang lässt sich im Setting Supermarkt aber nicht nur eine spezifische Vorgängigkeit des Vertrauens als Bedingung von Akzeptanz ausweisen. Für eine Befragte wird die Nutzung des Verfahrens auch zum ausdrücklichen Vertrauensbeweis und dies, obwohl sie kriminalistische Assoziationen zum Verfahren während des Einlesens ihrer Fingerabdrücke äußert, wie dem nachfolgenden Auszug aus dem Beobachtungsprotokoll zu entnehmen ist:

> Beobachtungsprotokoll Registrierung Erika Hundt, Sm: Der erste Versuch Frau Hundts Finger einzuscannen schlägt fehl. Der Filialleiter verändert daraufhin die Position des Fingers – offenbar erfolgreich, denn Frau Hundt kommentiert „Jetzt geht’s“. Sie schaut dabei sehr aufmerksam auf den Monitor. Die weiteren Scans weist der Fili-

> alleiter mit „nochmal“, „nochmal“, „nochmal“ an. Sie verlaufen offenbar ohne Fehler. Frau Hundt wirkt während des Einlesevorgangs ruhig und geduldig. Sie erzählt – unklar an wen gewandt – während des zweiten Scans, dass sie für den Personalausweis alle Finger habe einscannen lassen. Beim vierten Scan sagt sie zu ihrem Enkel, der neben ihr sitzt: „Jetzt sind wir in der Sünderkartei“, worauf der Enkel fragt, was dies sei, was Frau Hundt aber nicht erklärt.

Im späteren Interview auf diese Assoziation angesprochen, disqualifiziert Frau Hundt, ähnlich wie Frau Böttcher, die Assoziation *„Sünderkartei“* als *„Blödsinn“*, obwohl sie ihr Unbehagen zu explizieren weiß. Dabei stellt sie einen Zusammenhang zwischen der Erfassung ihrer Fingerabdrücke in der Einwohnermeldebehörde für ihren Personalausweis und einer polizeilichen Erfassung her „*weil man ja, der Fingerabdruck da auch registriert ist, ne? Dann. Ja ja. Aber gut, es war jetzt mehr Blödsinn, wie gesagt.“* Für ihre Nutzung im Supermarkt ist diese Assoziation gleichwohl unproblematisch, weil das Verfahren, besehen im Licht der Beziehung zum Fingerabdrucknehmer, eine andere Bedeutung erhält. Dass sich das Objekt Fingerabdruckverfahren gewissermaßen auch in den Eindruck auflöst, den es in einem bestimmten Augenblick, in einer ganz besonderen ‚Beleuchtung‘ macht, ist bereits in den heterogenen Zwecken ebenso angeklungen, wie auch in der Betrachtung zum relativen Wert des Datums Fingerabdrucks selbst. Frau Hundt nutzt das Verfahren hier nicht nur, weil sie von der Verlässlichkeit des Inhabers im Umgang mit den Daten überzeugt ist. Teilt auch sie eine gemeinsame Geschichte mit dem Supermarktbesitzer und habe diesem, auch nachdem die Familie den ersten kleinen Laden aufgegeben habe, *„die Treue weiter gehalten“* gründet sie die, gewiss geplante, Nutzung in einem expliziten Versprechen zur Nutzung gegenüber dem Besitzer:

> „((lacht)) Ja hab das ((unverständlich)) schon die ganze Zeit vorgehabt zu machen, aber dann war‘s meistens so, dass immer sehr viel Leut‘ an der Kasse war mit, da geht es dann immer schlecht, und dass ich das [die Werbung] denn gelesen hab und mit dem Besitzer, also dem Eigentümer, dem Herrn Boll dann drüber gesprochen hab, Abend vorher, und hab‘s gesagt, ‚für dich komm ich ma‘ ((lacht)). Aus dem Grund, da hab‘ ich Sie da gleich gesehen [Interviewerin am Informationsstand] und dann gleich drauf los.“

Neben den vorteilhaften Zwecken lässt sich das Motiv zur Nutzung des Verfahrens als Ausdruck ihrer anhaltenden Treue zum Supermarktbesitzer, hier, in Anlehnung an Marcel Mauss, der in seinem „Essai sur le don“ (1990) Elemente der Reziprozität, das heißt das Prinzip des Gebens und Nehmens (vgl. Adloff/Mau 2005)[62] beschreibt, dann auch als immaterielle Gabe

[62] Die Prinzipien des wechselseitigen Austausches von Leistung und Gegenleistung in sozialen Beziehungen ist ein klassisches soziologisches Thema, das sich mit der Frage nach der Integration von Gesellschaft beschäftigt, etwa: Aufgrund welcher Prinzipien handeln Menschen, wie bilden sich spezifische Strukturen wie z.B. Netz-

bestimmen, wie es selbst auch für das Vertrauen geltend gemacht werden kann: In „Das Geheimnis und die geheime Gesellschaft“ betont Georg Simmel (1992: 425), dass das Vertrauen, als das wesentliche Element der (geheimen) Gesellschaft, nicht „in demselben Maße verlangt werden (kann)“, wie es geschenkt wird. Dass Vertrauen gegeben, oder wie es auch heute nicht nur eine Redensart ist, „geschenkt“ wird, verweist geradezu, so auch Frauke Rischmüller (2012: 300), auf die Gabenformel des Vertrauens. Vertrauen, als Voraussetzung für die Etablierung sozialer Beziehungen, ergibt sich Mauss‘ Beobachtung nach daraus, dass jegliche Annahme einer Gabe von der Verpflichtung auf Gegenseitigkeit begleitet ist. Eine solche Norm etabliert sich jedoch unter Bedingungen der Unsicherheit – hat doch der Gebende keine Gewissheit darüber, ob und wie der Annehmende die Gabe erwidert. Erst im Vertrauen wird der Gebende handlungsfähig, da er so die Unsicherheit über das zukünftige Handeln seines Gegenübers aufhebt.[63] Dies lässt sich an den nachfolgenden Beispielen noch genauer ausführen.

Folgt man Martin Hartmann (2011: 24), wonach jenes sich Verlassen auf das Wohlwollen anderer, welches Anette Baier (2001) als den Kern des Vertrauens identifiziert, gleichsam sozialisiert ist, dann besteht die Gabe des Vertrauens auch darin, dass es nicht nur Beziehungen ermöglicht sowie gesellschaftlich als wertvoll erachtete Güter erhält. Dem Aufbau und Erhalt vertrauensvoller Beziehungen wird selbst ein eigener hoher Wert zugeschrieben, da „in dem Vertrauen des Menschen auf den andern […] ein ebenso hoher moralischer Wert [liegt], wie darin, dass diesem Vertrauen entsprochen wird“ (Simmel 1992: 425). Vertrauen lässt sich dann auch als eigenständiger Grund des Nutzungshandeln beschreiben, als ein Motiv, das sich am Gegenüber und eben an dieser Beziehung orientiert. In diesem Zusammenhang formuliert im Setting Einwohnermeldebehörde etwa auch das Ehepaar Janßen im Hinblick auf den staatlichen Umgang mit den Fingerabdruckdaten ein ausdrückliches Vertrauen, das einen vergleichsweise hohen Reflexionsgrad aufweist:

> Hans-Peter Janßen: „Also auf jeden Fall so, dass da nich‘ jeder Zugang zu hat. Dass das kontrolliert wird, und gewissenhaft kontrolliert wird, dass da nich‘ jeder Hans und Franz“
>
> Gudrun Janßen ((unterbricht)): „Genau.“
>
> Hans-Peter Janßen: „hingehen kann und sagen, ‚Hier, ich möchte da mal‘, durch n Anruf womöglich noch, ‚möchte da mal Klarheit haben. Schicken Sie mir mal ‘n paar Bilder zu‘. Also das“
>
> Gudrun Janßen ((unterbricht)): „Doch, da vertrau‘ ich schon drauf, dass da ordnungsgemäß mit umgegangen wird.“

werke oder Institutionen und welche Funktionen haben diese für die Gesellschaft und das gesellschaftliche Zusammenleben?

[63] In diesem Sinne, gleichwohl ohne expliziten Bezug, auch Luhmann (2000: 55): Vertrauen „will geschenkt und angenommen sein.“

> Hans-Peter Janßen: „dem muss ich schon vertrauen. Also, wenn ich da nich‘ vertrauen kann, denn, denn hab‘ ich überhaupt kein Vertrauen mehr.“

Abgesehen von der Erwartung, dass der Fingerabdruck sicher verwahrt und die im Prozedere der Antragstellung der neuen Ausweispapiere preisgegeben Daten nicht unbefugten Dritten verfügbar gemacht werden, bleiben die spezifischen Bedingungen, die für das Ehepaar die Vertrauenswürdigkeit signalisieren, im Interview implizit. Möglicherweise wird hier auch erst ex post ein vertrauensvolles Handeln expliziert. Anders als im Supermarkt sprechen diese Befragten jedoch nicht von vorgängigen Vertrauensgründen. Woran also macht sich das Vertrauen fest? Wie Systeme wie der Staat überhaupt Vertrauenswürdigkeit anzeigen, wird in der Literatur kontrovers diskutiert. In der Perspektive Luhmanns (2000) wie auch Giddens‘ (1995) besitzt ein Systemvertrauen, sei es in spezifische Rollenträger – Experten (vgl. Barber 1983 zum Arzt-Patienten-Verhältnis) oder kooperative Akteure (vgl. auch Coleman 1991) – oder in entpersonalisierte Systeme, etwa ‚die Wirtschaft‘ oder ‚den Staat‘, andere Qualitäten als personales Vertrauen. Anthony Giddens‘ Unterscheidung (1995: 102) zwischen „gesichtsabhängigen“ und „gesichtsunabhängigen“ Beziehungen verweist gleichwohl darauf, dass abstrakte Systeme auch immer über Zugangspunkte verfügen, an denen etwa der Bürger in den persönlichen Kontakt mit Vertretern des jeweiligen Systems gerät und an denen Vertrauen über persönliche Interaktion vermittelbar wird. Sie sind das „Bindeglied zwischen Personenvertrauen und Systemvertrauen“ (ebd.: 144), denn die „gesichtsunabhängigen“, unpersönlichen Zeichen für Vertrauenswürdigkeit geben in der Regel „nur in statistischer Weise ‚Widerworte‘, wenn sie nicht die von den Betreffenden angestrebten Ergebnisse liefern.“ (ebd.) Die Vertrautheit mit den offiziellen Prozeduren und den Interaktionen mit dem damit beauftragten Personal, von dem der oben zitierte Befragte erwartet, dass es etwa nicht auf telefonische Auskunftsersuchen reagiert, mag dann, im Sinne einer „Alltagsepistemologie“ (Hardin 2001) ein Vertrauen befördern, indem diese Erfahrungen auch auf abstrakte Systeme generalisiert werden.

Zudem wird das Vertrauen in den Staat durch das Ehepaar Janßen als ein eigenständiger Wert ausgewiesen, das mitunter als alternativlos erscheint, weil man *„vertrauen muss“.* Ein solches Erfordernis zu vertrauen betont auch ein anderer Befragter in der Einwohnermeldebehörde, der, zu seinen Erwartungen im behördlichen Umgang mit seinen Daten befragt, energisch formuliert: *„Wem soll man denn sonst noch vertrauen, wenn man schon da anfängt, der Behörde nich‘ zu vertrauen“* (Eberhard Pelzig, Einwo). Wird das Vertrauen in den Staat also im Sinne einer Verpflichtung generalisiert, die „jenseits ‚enger‘ partikularistischer Rahmen“ (Eisenstadt 2001: 336) liegt, legt dies eine Deutung nahe, wonach auch hier ein spezifisches Bin-

dungsmotiv – die Treue – zum Ausdruck gebracht wird. So liegt denn auch Dorothea Weltecke (2003: 74ff.) zufolge die wörtliche Bedeutung des „Vertrauens“ im Kontext einer spätmittelhochdeutschen Wortfamilie, zu der auch das Wort „treu“ gehört. Dabei ist Treue, so Simmel (2005: 97) ein Gefühl, das sich primär auf den Bestand einer Beziehung richtet. Es führt ein Eigenleben (ebd.: 99), das von einer Abwägung von Vor- und Nachteilen, die etwa mit der Fingerabdrucktechnologie in diesem Setting verbunden werden, zu entlasten vermag. Mit ihr wird dann auch eine grundsätzliche Achtung vor bzw. ein ehrerbietiges Vertrauen („deference“) in das Handeln staatlicher Behörden selbst zum Ausdruck gebracht. Dem „deference model of authority“ zufolge, so Tom Tyler (1998: 276), fügen sich die Bürger spezifischen Entscheidungen der Autoritäten nicht allein deshalb, weil sie von deren spezifischer Notwendigkeit überzeugt sind, sondern schlicht aus der Anerkennung der Legitimität der Autorität selbst, die im Fall des Ehepaar Janßen dann auch die legitime Adressierbarkeit ihrer Identität durch staatliche Behörden einschließt. Die Akzeptanz der Technologie lässt sich in diesen Fällen – vermittelt über ein generalisiertes staatliches Vertrauen – als unhinterfragte, mithin unhinterfragbare ausweisen.

Die Generalisierung des Vertrauens als einer spezifischen Haltung zum Staat ermöglicht dann auch die von David Easton (1975) beschriebene Unterstützung staatlichen Handelns. Denn während die Janßens explizite Vorteile thematisieren, die sich für sie aus der Aufnahme der Fingerabdrücke in die Ausweisdokumente ergeben, bleiben diese für Herrn Pelzig, der *„keine konkrete Situation vor Augen“* hat, die eine Identifizierung qua Fingerabdruck erforderlich mache, eher unklar. Ausgehend von der Frage, warum ein politisches System Bestandsfähigkeit aufweist, unterscheidet Easton (ebd.)[64] zwei Formen der bürgerlichen Unterstützung und konzipiert hierfür die Wahrnehmung von Ergebnissen politischen Handelns als Relevanzkriterium. Während sich die spezifische Unterstützung aufgrund einer Zufriedenheit der Bürger mit konkreten Ergebnissen politischen Handelns ergibt, bezieht sich die diffuse Unterstützung auf das Vertrauensobjekt selbst und auf die unmittelbaren Erfahrungen mit diesem:

> „Trust will be stimulated by the experiences that members have of the authorities over time [...]. In time, such sentiments may become detached from the authorities themselves and take the form of an autonomous or generalized sentiment towards all incumbent authorities and perhaps the regime as well.“ (ebd.: 448)

Danach kann die Zufriedenheit mit den wahrgenommenen politischen Leistungen für das eigene Leben ein allgemeines Gefühl nach sich ziehen, „that the authorities – meaning by this a succession of different sets of authorities as well as any current incumbents of office – can

[64] Zusammenfassend vgl. Fuchs (2002).

normally be trusted to take care of one's interests." (ebd.: 449) Das von den Befragten formulierte Vertrauen besitzt insofern einen intrinsischen Wert (in diesem Sinne v.a. Hartmann 2011, auch Baier 2001) und in diesen Fällen, so lässt sich schlussfolgern, bestätigt sich die Leistungsfähigkeit des abstrakten Systems darin, dass es in der Lage ist, Vertrauensbeziehungen herzustellen – setzt doch Vertrauen als Verhältnis, das sich um ein „anvertrautes" Gut etabliert, die Kooperation gerade voraus, indem auch derjenige, dem vertraut wird, sich auf die Vertrauenswürdigkeit und Kompetenz des Vertrauensgebers verlässt (vgl. Hartmann 2011: 240ff., Baier 2001). Diese Befragten suchen dann auch nicht aktiv nach Anzeichnen von Vertrauenswürdigkeit – und hierin zeigt sich wiederum der präreflexive Modus des Vertrauens –, sondern setzen diese vielmehr voraus, wie dann auch Frau Jeske (Einwo) betont:

> Susanne Jeske: „Ja, man muss mit meinen Daten, wenn ich sie jemanden anvertraue, schon sorgfältig umgehen. Sonst verliert man ja den Vertrauen in den Staat, oder in das Einkaufszentrum, wo man eingekauft hat oder in die Bank. Weil's nich' richtig geschützt ist oder ähnliches, weil 'ne Vertrauensbasis sollte da sein. Sonst wär'n Miteinander gar nich' möglich."
>
> I: „Und, sorgfältig umgehen, was, was meinen Sie dann, wofür sollte es?"
>
> Susanne Jeske: „Wenn man mir 'ne Katze anvertraut, dann lass ich sie auch nich' verhungern."

Aus dieser explizit moralischen Qualität des Vertrauens – des sorgfältigen „Kümmerns" um das An-Vertraute – ergibt sich für Frau Jeske zugleich ein verpflichtendes Moment, mit dem sie dann auch ihre eigene Fingerabdruckgabe im behördlichen Kontext verknüpft. In der expliziten Anerkennung staatlicher Kontrollmotive und einer Haltung, die die Geeignetheit des Verfahrens zur Umsetzung dieser anerkennt, ordnet sie die damit einhergehenden potentiellen Risiken – z.B. einer erneuten fälschlichen Verdächtigung oder nicht intendierter Verwendungen der Daten – ganz bewusst einem Vertrauen gegenüber staatlichem Handeln unter:

> I: „Sie sind, auf der einen Seite haben Sie diese Erfahrung gemacht, dass da Hausdurchsuchung waren, Sie mitverdächtigt oder miterfasst wurden und sagen, Ihr Vater ist bei der [unkonventionelle] Partei, engagiert sich und hier haben Sie aber gleich gesagt, ‚Ja, mach' ich', das is' eigentlich haben Sie gefühlt dagegen"
>
> Susanne Jeske ((fällt ins Wort)): „Ich bin schon immer 'n bisschen anders gewesen. Ich sag', jeder baut mal Scheiße. Aber man sollte den Leuten auch wieder vertrauen können. Bis zu 'nem gewissen Punkt. So. Ich versuch's jetzt, und vielleicht geh' ich jetzt als Beispiel für meine Eltern voran, und die machen das auch, weil sie merken, dass is' 'ne vernünftige Sache, wir unterstützen das doch. Vielleicht machen sie's nich'. So, aber irgendwer muss den Schritt wagen, und wenn nie einer mutig genug is', es zu tun, dann werden alle sagen, ‚Ne, ich hab' Schiss'. So."

Die Klassifizierung ihres Handelns als eines mit Vorbildcharakter qualifiziert als ausdrückliche Gabe unter der Maßgabe einer gegenseitigen Selbststeigerung von Vertrauen, mit der sie,

nicht nur trotz, sondern vor allem aufgrund faktischer Einwände, die etwa in ihrem persönlichen Umfeld gegen die Nutzung des Verfahrens eingebracht werden, ausdrücklich Vertrauen in staatliches Handeln anzeigen will. Zentraler Bezugspunkt ihres Handelns und gleichsam politischen Urteilsbildung ist ein grundsätzliches Vertrauen in die Leistungsfähigkeit des politischen Systems. Es verbindet sich in diesem Fall im Geben des Vertrauens dann auch ein normatives Moment, weil es, wie es Luhmann (2000: 55) formuliert, ermöglicht, den anderen in seinen „Bann zu ziehen", indem es die Erwartung transportiert, dass dieses Vertrauen nicht enttäuscht wird: „Der Prozeß [des Vertrauens] beginnt mit einer riskanten Vorleistung, die als Wagnis schlecht normiert werden kann, sondern eher dem Verhalten von Helden oder Heldinnen ähnelt." (ebd.)

3.2.3 Zusammenfassende Überlegungen

Steht in deskriptiver Hinsicht die Abwesenheit von Freiwilligkeit für eine fehlende Freiheit nach der Maßgabe des eigenen Willens zu handeln, dann folgt dies aus der normativen Idee, dass mit Entscheidungs- und Handlungsfreiheit die Möglichkeit zur Selbstbestimmung gegeben sein soll (vgl. Ladwig 2006). Die Ergebnisse zeigen, dass sich Vorstellungen von Freiwilligkeit und Zwang und gleichsam Akzeptanz aber nicht zwangsläufig an faktischen Bedingungen festmachen lassen. Sie sind sowohl abhängig von konkreten wie auch wahrgenommenen Handlungsalternativen und dazu gehören dann nicht nur die Verfügbarkeit alternativer Zahlungs- oder Zugangsmittel, sondern mitunter auch die räumliche Distanz zur nächstgelegenen Videothek, die ohne Fingerabdruckverfahren funktioniert. Die Relevanz der insofern jeweils „tragbaren Opportunitätskosten" (ebd.: 90) variiert, erstens, weiter mit der persönlichen Relevanz der Zwecke der Technologie in den Settings, sowie zweitens, mit den Bedingungen einer konkreten Situation, die überhaupt erst Assoziationen hervorrufen und Haltungen buchstäblich erst entstehen lassen. Vor allem der Einfluss situativer Zwänge macht darauf aufmerksam, dass sich von beobachtbaren Handlungen kaum eindeutig auf Akzeptanz oder ihr Fehlen schließen lässt. Akzeptanz hat, anders als es Doris Lucke (1995: 394, Herv. i.O.) formuliert nicht immer „von außen beobachtbare […] *Handlungskonsequenzen.*" Und auch ausdrückliche Ablehnung ist als solche nicht immer zu identifizieren. Akzeptanzbedingungen generieren sich, drittens, erst in Abhängigkeit davon, welche Bedeutung den biometrischen Daten im jeweiligen Setting zugeschrieben wird und welche entsprechende Abwägungen über Vor- und Nachteile überhaupt erst erforderlich macht. Ob das Fingerabdruckverfahren als eine problematische Kontrolltechnologie wahrgenommen wird, erweist sich, viertens, dann

davon abhängig, ob es mit den in einem Setting etablierten Verhältnissen und darin eingelassenen Werten kollidiert. Dies konkretisiert die Bedingungen der von den Befragten formulierten ambivalenten Haltung gegenüber dem Verfahren auch im Hinblick auf seine möglichen Risiken. Vor diesem Hintergrund zeigt sich dann auch, dass ein Ergründen von Haltungen zu Kontrolltechnologien und ihrer Akzeptanz sich auch als eine Frage danach erweist, „what is exposed, why and how" (Ball 2009: 653). Seinen exemplarischen und wohl ausdrücklichsten Beleg findet dies in der Haltung des 65-jährigen Peter Wagner (Sm), der auf die Frage danach, ob es Daten gibt, die für ihn eine besondere Bedeutung haben – „vielleicht besonders privat sind, die Sie nicht so ohne weiteres angeben würden?" – antwortet: *„Es kommt drauf an, nein, das kann ich so nicht sagen, es kommt darauf an, wer sie haben will. Und wofür."*

Mit dem Vertrauen werden, zuletzt, für die Bestimmung der Akzeptanz zwischen Objekt, Subjekt und Kontext konkrete Beziehungen und in ihnen angelegte Regeln in dieses Verhältnis eingeführt, die, wie gezeigt, selbst motivierend für die Nutzung einer ambivalenten Technologie sein können. Dabei liegt die Besonderheit des Vertrauens, sei es implizit, das heißt vorgängig, sukzessive situativ erworben oder ausdrücklich reflexiv, darin, dass die Risiken, die sich zumindest theoretisch aus der Nutzung der Technologie ergeben könnten und die sich konkret durch „Entkopplungs- und Zurechnungsprobleme" (Bonß 1996: 178) auszeichnen, weder für die Gegenwart, noch für die Zukunft im Rahmen dieses Verhältnisses erwartet werden.[65]

Die Ergebnisse zeigen, dass Risiken im Vertrauen mitunter affektiv überdeckt werden, weil es die Befragten in eine Haltung von Normalität und Risikofreiheit versetzt. Das affektive Moment des Vertrauens ist unter anderem von Karen Jones (1996) und Bernd Lahno (2002) betont worden, wonach Vertrauen – als eine emotionale Einstellung – „bestimmte Interpretationsmuster nahe" legt (Lahno ebd.: 13) und damit die Wahrnehmung leitet. Es bestimmt sich durch eine „teilnehmende Haltung" (ebd.: 209) – hier gegenüber dem Fingerabdrucknehmer – und basiert auf einem „Gefühl der Verbundenheit" (ebd.: 209), das insofern auch Handlungsbereitschaften nach sich zieht (vgl. hierzu auch Frevert 2013: 21ff.), weil es, im Sinne einer

[65] Der Bezug auf Risiken innerhalb des Vertrauenskonzeptes wird gleichwohl kontrovers diskutiert und macht sich vor allem an der Bestimmung der Reflexivität fest, mit der Risiken Eingang in vertrauensvolles Handeln finden (vgl. z.B. die Kritik an Baiers Konzept bei Lagerspetz 2001: 101ff.). Vergleichbares gilt auch für die Auseinandersetzung Martin Endreß (2001) mit dem Luhmannschen Vertrautheitsbegriff, die darauf zielt, das Vertrauen von einer Entscheidung unter reflexiv abgewogenen Risikobedingungen abzugrenzen. Allerdings lässt sich das Risiko der Vertrauenshandlung bei Luhmann (2000: 23) auch darin entdecken, dass es in „einem Überziehen der Informationen dieser Vergangenheit" (2000: 23) besteht, weil sich, analog zur Bestimmung des Vertrauens bei Anette Baier (2001), angesichts der Freiheit des Gegenübers, Zukunft gleichwohl auch immer anders darstellen kann. Sowohl in der Bestimmung von Baier (2001), Luhmann (2001) als auch Endreß (2001) liegt das Spezifische in der Paradoxie, dass in der vertrauensvollen Haltung die (riskanten) Möglichkeiten zugleich vorhanden wie auch ausgeschlossen (als „Erfahrung der Negation", Endreß 2001: 184) sind.

„attitude of optimism“ (Jones 1996: 5), die Befragten davon ausgehen lässt, dass sich andere, von denen man zumindest in Teilen abhängig ist, sich im Bedarfsfall wohlwollend verhalten.

Der im Laufe des 20. Jahrhunderts begonnene Diskurs um Technisierung und die Folgen des Technologieneinsatzes, das heißt die Kontroverse darüber, dass das, was technisch machbar ist, mitunter auch realisiert wird und dann auch Zumutungen und Betroffenheiten mit sich bringt, hat das Vertrauen schon früh zu einem Aspekt der Akzeptanzforschung werden lassen. Die zunehmende Komplexität von Technologien und damit verknüpfte Fragen der Zurechenbarkeiten von Risiken führten dazu, dass sich Menschen zunehmend auf die Glaubwürdigkeit Dritter verlassen müssen, die Informationen über diese bereitstellen (vgl. Renn 2010). Dabei gerät die Funktion der Vertrauensfrage im Kontext einer akzeptanzorientierten Technikgestaltung regelmäßig zum Requisit der Akzeptanzforschung, da sie, ihrem lateinischen Begriffsursprung „‚requīsītum‘ – (auf)suchen, verlangen, nachfragen, nachforschen, fordern“ (Pfeifer et al. 1993) folgend, im Rahmen einer akzeptanzorientierten Technikgestaltung auf eben das ‚Erforderliche‘ reduziert wird, das beschafft werden muss. Die Frage nach dem Vertrauen als zu Beschaffendes erweist sich damit als ein „Effekt zweiter Ordnung“ (Grunwald 2003: 115 zit. in Petermann/Scherz 2005: 50) – gilt es doch als das Produkt einer deliberativen Akzeptabilitätspolitik, welche darauf zielt, dass „über eine offene wissensbasierte und ethisch orientierte gesellschaftliche Diskussion‘ […] Vertrauen geschaffen [wird].“ (ebd.) Vor allem im Zusammenhang mit der Idee des partnerschaftlichen Austausches zwischen Laien und Experten (vgl. Wiedemann/Mertens 2005: 42) und damit hinsichtlich der Akzeptanz unterschiedlicher Wissensformen, resp. der Risikokommunikation, wird das Vertrauen als erforderlich für die Akzeptanz etwa umstrittener politischer Entscheidungen oder kontroverser Maßnahmen konzipiert. Michael Siegrist (2001: 21) etwa bestimmt das Vertrauen zwischen Bürgern und Experten als einen wesentlichen Einflussfaktor für die grundsätzliche Perzeption von „wahrgenommenen Risiken oder Akzeptanz einer Technologie“. Dabei handelt es sich um einen Zusammenhang, der sich im Hinblick auf die Ergebnisse der vorliegenden Studie insofern als ambivalent ausweisen lässt, weil sich, wie dargestellt, zwar eine Glaubwürdigkeit der sich sowohl im Risiko- als auch im Sicherheitsdiskurs entfaltenden Argumente ausmachen lässt. Die im kritischen bzw. Datenschutzdiskurs angeführte Forderung zur Datensparsamkeit findet ihre Grenzen jedoch im technischen Wissen und scheint auch weniger eindeutige Gewissheiten zu etablieren, weil sie sich der gleichen irritierenden Momente des zukünftig Bedrohlichen wie des Sicherheitsdiskurses bedient. Die Bedeutung des Vertrauens für die Akzeptanz hat sich demgegenüber als ein Modus erwiesen, mit dem sich das daraus resultierende gefühlte Unbehagen vielmehr auflösen lässt.

Das Nutzungshandeln ist insofern komplex motiviert, neben situativen Zwängen und etablierten Routinen lassen sich Vertrautheit und Vertrauen selbst als seine Bedingungen ausweisen. Zieht das Vertrauen zudem seine Wirkung daraus, dass es auf umfassendes Wissen verzichtet, ermöglicht es den Befragten, die unheimlichen Möglichkeiten der Datenverwendung auszublenden. Es beruht dann eben nicht auf einem spezifischen Wissen, etwa zu den konkreten Umständen der Datenspeicherung und -verwendung. In der Regel haben die Befragten wenig Kenntnis hierüber und fordern ein solches Wissen auch nicht ein. Vielmehr werden ‚schlicht' die vergangenen (positiven) Erfahrungen mit den Fingerabdrucknehmern für die Zukunft generalisiert. Das Vorhandensein von Vertrauen steht folglich in einem Zusammenhang mit der Einschätzung des Risikos (vgl. hierzu Hardin 2001: 315), was sich dann auch darin zeigt, dass die dargestellt vertrauensgeneigten bzw. -motivierten Befragten eine vergleichsweise geringer ausgeprägte ambivalente Haltung gegenüber der Technologie aufweisen als andere Befragte, denen es dann auch in geringerem Maße gelingt, die mit der Technologie verbundene Ambivalenz für sich aufzulösen.

3.3 Akzeptanz im Verhältnis von Vertrauen und Misstrauen

„Nicht jede Unstimmigkeit weckt Zweifel an den vertrauten Zügen der Umwelt, nicht jede Enttäuschung zerstört das Vertrauen. Eben deshalb muss es aber eine Grenze geben, wo die Absorptionskraft endet, wo Vertrautheit oder Vertrauen abrupt in Mißtrauen umschlagen." (Luhmann 2000: 97)

Ebenso wie Akzeptanz ist Vertrauen nicht statisch, sondern kontextuell und situativ variabel. Obwohl die Studie nicht darauf angelegt war, explizit Vertrauenshaltungen als Bedingung der Akzeptanz zu eruieren, haben sich im Hinblick auf die Akzeptanz unterschiedliche Positionen im jeweiligen Verhältnis von Datengeber und -nehmer und in diesem Zusammenhang auch unterschiedliche Vertrauenserwartungen, und -erfordernisse als relevant erwiesen. Aus diesem Grund gilt es daher nachfolgend diese Verhältnisse noch einmal genauer für jene Fälle in Augenschein zu nehmen, in denen sich die Ambivalenzen, die mit der Fingerabdruckgabe verbunden werden, für Befragte nicht auflösen lassen. Denn während Vertrauen, auf der einen Seite, in bestimmten Kontexten, und eingebettet in spezifische Verhältnisse, die Akzeptanz der Technologie befördert, wird sie in anderen Kontexten, zum einen, als konkreter Ausdruck für ein Misstrauen gedeutet. Zum anderen zeigt sich, dass für Befragte mit einem misstrauischen Blick auf die potentiellen Risiken, die sich aus der Preisgabe des Fingerabdrucks ergeben könnten, das Vertrauen in den Fingerabdrucknehmer trotz persönlicher Vorteile und einer Anerkennung legitimer Kontrollzwecke als ambivalent zu charakterisieren ist. Zu diesem

Zweck richtet sich der Blick im Folgenden auf empirische Ergebnisse der Akzeptanzforschung zu Sicherheits- und Kontrolltechnologien, den Zusammenhang von Vertrauen, Misstrauen und Biometrie und damit Einsichten, die unter Bezugnahme auf ein in der vorliegenden Studie von den Befragten ausgedrücktes (fehlendes) Vertrauen oder Misstrauen im Verhältnis zum Fingerabdrucknehmer konkretisiert werden sollen.[66]

3.3.1 Exkurs 1: Vertrauen in der Akzeptanzforschung zu Sicherheitstechnologien

Etabliert sich mit der Invisibilisierung sachtechnischer Abläufe eine Eigenmacht der differenzierten Experten- und Techniksysteme, dann unterscheidet Gerald Wagner (1994) mit Max Weber zwischen dem Einverständnis in die rationale Ordnung und dem Verständnis ihrer Komplexität. So charakterisiert Wagner (ebd.: 145) die „Risikogesellschaft“ auch als „Vertrauensgesellschaft“, denn in der „Einverständnisgemeinschaft“ *muss* die Nicht-Universalisierung des Wissens […] durch die Universalität des Vertrauens kompensiert werden.“ (ebd. 148). Technologisch bedingte Nebenfolgen allerdings rufen Glaubwürdigkeitsdefizite hervor. Im Kontext von Risikodebatten entwickeln sich folglich Vertrauensfragen dann auch im Hinblick auf Institutionen und ihre Vertreter. Es geht mithin um ein sogenanntes öffentliches Vertrauen. Das Risiko bei neuen Sicherheits- und Kontrolltechnologien ist dabei doppelt verortet: Zum einen jenes, das durch ihren Einsatz selbst generiert wird und, zum anderen, ein Risiko, auf das die neuen Technologien eine Antwort bereitstellen sollen. Wird nun in empirischen Untersuchungen das Verhältnis zwischen den die Daten preisgebenden und den Daten erhebenden Akteuren beleuchtet, dient das in letztere gesetzte Vertrauen als ein indirekter Indikator der Akzeptanz. Das hinsichtlich der Akzeptanz von biometrischen Technologien zu untersuchende Verhältnis ist dabei durch die in Kapitel 1.2.2 vorgestellte Akzeptanzheuristik und die dort entworfenen Rollen fixiert: Sind in Bezug auf biometrische Technologien privatwirtschaftliche Anwendungen auf die „individuelle Akzeptanz“ der Konsumenten gerichtet, gilt das Vertrauen in die jeweiligen Betreiber einer Technologie und mithin die Erwartung, dass diese die mit ihr verbundenen potentiellen Risiken nicht zum Nachteil der Anwender nutzen, als Determinante für die Nutzungsabsicht einer Technologie: (z.B. Königsdorfer 2008: 42 mit Bezug auf Dahlberg/Malat/Öörni 2003). Demgegenüber wird bei der Einführung von Sicherheitstechnologien, wie biometrischer Merkmale in nationale Identitätsdo-

[66] Eingang in die nachfolgenden Darstellungen finden in überarbeiteter Form veröffentliche Ausführungen zum Vertrauen, die als Gemeinschaftsarbeit unter dem Titel „Die gesellschaftliche Konstruktion der Sicherheit“ (Krasmann et al. 2014), sowie 2015 unter dem Titel „Gambling with the ‚Gift‘?“ (Kühne 2015) erschienen sind.

kumente, im Rahmen einer gesellschaftlichen Akzeptanz das Verhältnis der Bürger zum Staat bzw. der mit der Verwendung der Daten beauftragten Stellen befragt. Empirisch zeigt sich diese Perspektive dann etwa darin, dass das Vertrauen, auf der einen Seite, zum Faktor der Akzeptanz wird, welches, über die Erwartungen an die Vertrauens- und Glaubwürdigkeit der den Technikimplementationsprozess gestaltenden Personen (Schäfer/Keppler 2013: 27) bzw. deren wahrgenommene Befähigung Risiken zu kontrollieren und zu beherrschen, die Wahrnehmung von Risiken selbst moderiert (vgl. Renn 1993: 69). In den Studien, die der gesellschaftlichen Akzeptanz von Biometrie nachgehen, steht, wie nachfolgend in Tabelle 12 exemplarisch aufgeführt, die Frage nach der Einschätzung der Vertrauenswürdigkeit im Umgang mit den erhobenen Daten (Lüdemann/Schlepper 2013, Bug/Wagner 2015, Bug/Münch 2012) durch den bzw. die die Daten erhebenden Akteur(e) im Mittelpunkt. Die Rolle des Vertrauens steht in diesen Studien im Fokus, um die Auswirkungen staatlichen Sicherheitshandelns seit 2001 in Deutschland zu ermitteln und ist dementsprechend kontextualisiert. Zu diesen Untersuchungen gehören die Studie „Der ‚überwachte Bürger' zwischen Apathie und Protest" (z.B. Schlepper/Lüdemann 2010) und die Untersuchungen im Teilprojekt „Der Einfluss institutioneller Regimes auf die Billigung sicherheitspolitischer Maßnahmen" des Forschungsverbundes SIRA (z.B. Bug/Münch 2012, Bug/Wagner 2015). Im Rahmen dieser Untersuchungen wurden die Befragten gebeten anzugeben, inwieweit sie davon ausgehen bzw. daran glauben, dass die Betreiber oder Behörden mit den erfassten Daten vertrauenswürdig umgehen.

Tabelle 12: Glaube an einen vertrauenswürdigen Datenumgang durch die Behörden

	ja, auf jeden Fall	*eher ja*	*eher nein*	*nein, auf keinen Fall*
Glauben Sie, dass Behörden mit Ihren Ausweis-, Telefon-, Passagier-, Bank- und Internetdaten vertrauenswürdig umgehen? (ISIP-Projekt, eigene Berechnungen, N = 2.176)	7,9%	36,1%	39%	15,8%
Gehen Sie davon aus, dass Behörden im Rahmen der Vorratsdatenspeicherung mit ihren Telefon- und Internetdaten vertrauenswürdig umgehen? (Bug/Münch 2012: 169f., N = k.A.)[67]	7,1%	43,3%	k.A. [68]	15,6%
(Passagierdaten) *Gehen Sie davon aus, dass Behörden mit den Daten vertrauenswürdig umgehen?* (Bug/Wagner 2013, N = 378)[69]	19,6%	52,1%	22,2%	5,8%

Quelle: Krasmann et al. 2014: 114

Woran ein vertrauenswürdiger Umgang gemessen wird, lässt sich im Rahmen dieser Befragungen jedoch nicht ermitteln, sodass sich das in den Ergebnissen andeutende Unbehagen – wenigstens ein Drittel der jeweils Befragten hält einen nicht vertrauenswürdigen Umgang mit den Daten für wahrscheinlich – unbeschrieben bleibt. Fraglich erscheint ebenso, ob die Bewertung der Vertrauenswürdigkeit selbst einen Indikator für Vertrauen in den jeweiligen Akteur darstellt, sich also daraus ein Vertrauensverlust oder fehlendes Vertrauen oder gar Misstrauen ableiten lässt. Möglicherweise wird hier zunächst nicht mehr als eine antizipierte Diskrepanz zwischen dem angekündigten Handeln der Institution und den Vorstellungen oder Erfahrungen darüber, welche Zwecken diese tatsächlich verfolgt bzw. verfolgen könnte, erfragt. Erfasst wird insofern das Ausmaß einer „informationellen Angst" (Capurro 2008: 53), in der trotz vielfältiger Faktenlagen für die Bürger die Unsicherheit bleibt, ob diesen Informationen zu trauen ist, aber weniger der Grad eines Vertrauensverhältnisses. Ergänzen ließe sich vor dem Hintergrund der vorliegenden Studie, inwiefern hier auch Abhängigkeiten im Hinblick auf die grundsätzliche Legitimität der Erfassung von Daten sowie Vorstellungen ihrer legitimen Verwendung existieren, die sich wiederum erst in spezifischen Verhältnissen entfalten. Die Relevanz letzterer wird gleichwohl angedeutet: Denn inwiefern den Befragten ein potentiell missbräuchlicher Umgang mit den Daten vorstellbar erscheint, variiert je nach dem

[67] Diese Frage wurde dem Teil der Gesamtstichprobe (1.257 Befragte) gestellt, die die Frage, ob sie bereits von der Vorratsdatenspeicherung gehört hätten, bejahten. Dies entspricht einem Anteil von 81,2 Prozent an der Gesamtstichprobe (Bug/Münch 2012: 166), eine genaue Zahl ist dem Beitrag jedoch nicht zu entnehmen.

[68] Dem Beitrag von Bug und Münch (2012) sind differenzierte Zahlen zu den Antwortkategorien *eher nein* und *nein, auf keinen Fall* nicht direkt zu entnehmen. 15,6 Prozent bezeichnen die Autoren als „die sehr kritische Gruppe" (ebd.: 170), sodass hier davon ausgegangen wird, dass es sich dabei um die Personengruppe handelt, die die Kategorie *nein, auf keinen Fall* angaben.

[69] Befragt wurden nur Passagiere mit Vorwissen zur Fluggastdatenspeicherung (N = 378).

Kontext, in dem persönliche Daten preisgegeben werden. Die Ergebnisse der Studien zeigen, dass verschiedenen Akteuren eine unterschiedliche Vertrauenswürdigkeit im Umgang mit diesen Daten zugeschrieben wird. Die in Tabelle 13 dargestellten Ergebnisse aus dem SIRA-Projekt etwa verdeutlichen, dass Befragte eher von einem nicht vertrauenswürdigen Umgang mit den Daten durch Kommunikations- oder Verkehrsunternehmen als durch Behörden ausgehen.

Tabelle 13: Glaube an einen vertrauenswürdigen Umgang mit erhobenen Daten durch staatliche und nicht-staatliche Institutionen

Gehen Sie davon aus, dass Behörden im Rahmen der Vorratsdatenspeicherung mit ihren Telefon- und Internetdaten vertrauenswürdig umgehen? (Bug/Münch 2012: 169f.)	15,6% Ablehnung (*nein, auf keinen Fall*)
Gehen Sie davon aus, dass Kommunikationsunternehmen im Rahmen der Vorratsdatenspeicherung mit ihren Telefon- und Internetdaten vertrauenswürdig umgehen? (Bug/Münch 2012: 169)	26,8% Ablehnung (nein, auf keinen Fall)
(Passagierdaten) Gehen Sie davon aus, dass Behörden mit den Daten vertrauenswürdig umgehen? (Bug/Wagner 2013)	5,8 % Ablehnung (nein, auf keinen Fall)
(Passagierdaten) Gehen Sie davon aus, dass Verkehrsunternehmen mit den Daten vertrauenswürdig umgehen? (Bug/Wagner 2013)	7,1% Ablehnung (*nein, auf keinen Fall*)

Quelle: Krasmann et al. 2014: 116

In der Studie von Lüdemann und Schlepper (2013) wird unter Bezug auf das Konzept der „procedural utility“ (Frey et al. 2004), das auf Fragen der Gerechtigkeit und Fairness zielt, die Frage nach der Vertrauenswürdigkeit theoretisch fundiert und offengelegt, dass sie auf das Ausmaß zielt, in dem die „Bürger das Gefühl haben, dass staatliche Maßnahmen ihre Autonomie und Freiheit sowie ihr Bedürfnis nach Selbstbestimmung respektieren und [die Maßnahmen] zeigen, dass der Staat seinen Bürgern vertraut.“ (Lüdemann/Schlepper 2013: 152f.) Im politikwissenschaftlichen Denken hat die Annahme, dass die Unterstützung der Bevölkerung für den Bestandserhalt eines politischen Systems von zentraler Bedeutung ist, eine lange Tradition und baut auf der Annahme auf, dass eine effektive Arbeit der Regierung sich auf die Vertrauensbasis der Bevölkerung stützt (vgl. z.B. Gabriel 1993). Der Zweck dieser Forschung zum Systemvertrauen wird darin gesehen, dass Vertrauen in staatliches Handeln konstitutiv für die Stabilität politischer Systeme ist. Der unter anderem aus der Governance-Forschung (Easton 1975) stammenden, primär auf die Legitimierung staatlichen Handelns zielenden, Prämisse folgend, dass die Bürger sich dann gut regiert fühlen, dem Staat vertrauen und folglich bereit sind, (unterstützende) Gegenleistungen zu erbringen, wenn sie die staatliche Performanz, das heißt die „Leistungen“ des Staates als hoch einschätzen, beziehen die Autoren

der Studie dann auch die Vertrauenseinstellungen der Bürger – sowohl spezifisch in den Staat als auch als ein generelles Vertrauen – in ihre Untersuchung mit ein (vgl. Tabelle 14).

Tabelle 14: Häufigkeiten der Antworten auf die Frage nach dem „Vertrauen in die Regierung“

Antwortkategorie	*N*	*%*
sehr großes Vertrauen	61	2,8
großes Vertrauen	783	36,0
geringes Vertrauen	1136	52,2
überhaupt kein Vertrauen	179	8,2
weiß nicht	16	0,7
verweigert	1	0
Summe	2176	100

Quelle: Schlepper/Lüdemann 2010: 573

Die Ergebnisse der Studie zeigen, dass je geringer der Nutzen der Maßnahmen eingeschätzt wird, umso geringer auch das Vertrauen in die Regierung (zu weiteren Einflussfaktoren siehe Schlepper/Lüdemann 2010) ist. Umgekehrt, so das Ergebnis der Studie, stärkt eine positiv bewertete Performanz staatlichen Handelns auch das Vertrauen in die Regierung – ein Zusammenhang der sich in der vorliegenden Studie auch bei den ausdrücklich vertrauenden Befragten (vgl. Kapitel 3.2.2.2.3) im behördlichen Setting andeutet.

Gleichwohl hat sich gezeigt, dass sich ein Vertrauen in staatliches Handeln auch abgekoppelt von einer spezifischen Leistung, die mit spezifischen Technologien verbunden wird, erweisen kann und Nutzungszwecke nicht immer auch auf ein persönlich relevantes Interesse zurückgeführt werden können. Zudem sind die in dieser Studie verwendeten generalisierenden Fragen zum Vertrauen kritisch zu bewerten: etwa *„Wieviel Vertrauen haben Sie in die Regierung“* oder *„Inwiefern würden Sie der folgenden Aussage ‚Den meisten Menschen kann man vertrauen‘ zustimmen“*. Sie verlangen den Befragten, gleichsam trotz und ungeachtet der ex ante gebildeten Hypothesen über Zusammenhänge des Vertrauens, im Moment der Fragestellung eine „Abstraktion von Sozialbeziehungen“ ab (Fuhse 2002: 424). Die Idee einer generellen Vertrauenseinstellung, die sich hinter der Aufforderung zu einer solchen Beurteilung verbirgt, provoziert, wenn die Frage zufriedenstellend beantwortet werden soll, die Gegenfrage: „wobei?“ (ebd., hier zur Problematik von Fragen, wie „kann man Menschen im Allgemeinen vertrauen?). Diese Bedeutung der Relativität der Verhältnisse ist dann auch in Kapitel 3.2.2 belegt worden. Und selbst wenn das Vertrauen in den Untersuchungen als ein spezifisch vermittelnder Faktor in den in Frage stehenden (Akzeptanz-)Verhältnissen und mithin der Akzep-

tanzbilanz (etwa Nutzen vs. Risiko des konkreten Datenmissbrauchs) adressiert wird, steht, nicht zuletzt, in Frage, ob eine solche Frage fehlendes Vertrauen womöglich nicht erst kommuniziert – ein Einwand, den sich gleichwohl auch die vorliegende Studie gefallen lassen muss.

3.3.2 Exkurs 2: Zum Zusammenhang von Vertrauen, Misstrauen und Biometrie

In den vergangenen Jahren ist zudem der Zusammenhang von Vertrauen, Misstrauen und neuen Informationstechnologien vermehrt in den Fokus der Betrachtung gerückt und wird im Hinblick auf ihre Nutzung, mithin ihre Akzeptanz, als zunehmendes Sich-Verlassen auf, mitunter ein Vertrauen in, Überwachung ermöglichende Technologien problematisiert. Nun lässt sich mit Bezug auf Georg Simmel (1992, 1989) oder Anthony Giddens (1995) einwenden, dass das Vertrauen in Technologien unter Bedingungen moderner Komplexität immer schon eine Vorbedingung für die Entstehung von Überwachung war. Zum einen basiert moderne Staatlichkeit auf der systematischen Erfassung von Daten über die Bevölkerung und eine so auch als Monitoring verstandene Überwachung ist gleichsam ihr Konstituens (Krasmann 2004). Unter einer entwicklungstheoretischen Perspektive führt dies, zum anderen, auch entlang einer Veränderung der Vertrautheit im Sinne sinn- und deutungsstiftender Umweltelemente und bezieht sich insofern auf eine Veränderung von Vertrauensformen im Modernisierungsvollzug, wie sie etwa Niklas Luhmann ausführlich (2000) beschrieben hat. Im Mittelpunkt dieser Betrachtungen steht die Veränderung der gesellschaftsintegrativen Bedingungen für Selbstverständlichkeit und Gewohnheit aufgrund eines Bedeutungsverlustes von ehemals sinnstiftenden Institutionen wie Religion und Tradition. Lösen sich in differenzierten Sozialordnungen die vormals engen Grenzen der vertrauten Welt auf (Giddens 1995: 33ff.), dann sind nicht länger die vor allem auf persönlichem Kontakt basierenden Vertrauensverhältnisse hinreichend für die Lebensbewältigung. Mit zunehmender gesellschaftlicher Differenzierung etabliert sich vielmehr ein sogenanntes „versachlichtes Vertrauen“ (Endreß 2002: 14, vgl. Simmel 1992: 394) oder „Systemvertrauen“ (Luhmann 2000: 60ff.). Verbindlichkeiten zwischen Interaktionspartnern etwa verlagern sich zunehmend auch auf symbolische Zeichen (Simmel 1989: 216) oder „Kommunikationsmedien“ (Luhmann 2000: 60ff.) und mit ihnen ein Vertrauen auf das Funktionieren in die differenzierten Elemente des Gesellschaftssystems. Symbolische Elemente wie das Geld bündeln Komplexität – erhält der Einzelne doch „durch Geld mithin die Komplexität des gesamten Wirtschaftssystems […] buchstäblich in die Hand“ (Luhmann 2000:

63). Symbole dienen in diesem Sinne dazu, das Unvertraute ins Vertraute zu überführen und dieses so zum Teil der Lebenswelt werden zu lassen, denn

> „sie setzen die Differenz zwischen Vertrautem und Unvertrautem voraus, und sie funktionieren in der Weise, dass sie den Wiedereintritt dieser Differenz in das Vertraute ermöglichen." (Luhmann 2001: 145)

Als Form der „Selbstreferenz" (Luhmann 2001: 146) reduzieren sie Komplexität in dem Maße, wie sie die Bedingungen des Handelns in sich selbst generieren, und die insofern nicht mehr ausgehandelt werden müssen. Mit der Entpersonalisierung sozialer Kontakte wird Verbindlichkeit neben den symbolischen Zeichen zudem durch die Installierung von Expertensystemen geschaffen. Dieser zweite Entbettungsmechanismus der Moderne (Giddens 1995: 34), den Luhmann als die „Generalisierung von Kommunikationsmedien" verhandelt (Luhmann 2000: 66), fungiert als zunehmende Entpersonalisierung funktionaler Rollenträger, die Wissen bündeln. Ein (sachliches) Vertrauen bezieht sich in diesem Sinne weniger auf ihre personale Identität, als vielmehr auf entsprechende Sachkenntnis und spezifische Kompetenzen (Giddens 1995: 39) bzw. auf die technische Leistungsfähigkeit technologischer Medien. Mit zunehmender Differenzierung in einer Gesellschaft von Fremden, in der soziales Handeln nicht mehr durch rein persönliches Aushandeln möglich ist, übernehmen folglich Institutionen Vertrauensleistungen und neue „symbolische Zeichen" (Simmel 1989: 216) oder „tokens of trust" (Lyon 2001: 27) gewinnen an Bedeutung. Identitätsdokumente oder andere ‚Beweise' dafür, wer jemand ist (ebd.) oder auch die Verankerung staatlichen Handelns im Recht (Luhmann 2000: 77) ersetzten das fehlende Wissen über die Motive anderer, das heißt neben personales Vertrauen tritt ein versachlichtes oder institutionelles Vertrauen (vgl. dazu auch Giddens 1995, Luhmann 2000). Institutionalisierte Kontrollmechanismen ermöglichen dort, wo sie etabliert werden, den Verzicht auf weitere Kontrollerfordernisse, sodass sich (personales und institutionelles) Vertrauen als kulturelle Ressource etablieren kann (vgl. Sztompka 1998). Für das Verhältnis zwischen Bürger und Staat bedeutet dies eine Übertragung von Kontrolloptionen, die das Risiko des sich Anvertrauens aufheben und freies Handeln ermöglichen. Für das „treuhänderische Verhältnis" (Locke 1974: 115 zit. in Hartmann 2002: 386) zwischen Bürger und Staat etwa, so fasst es John Locke (1977) in seiner Zweiten Abhandlung über die Regierung, bedeutet dies für das Ineinandergreifen von Vertrauen und Kontrolle zweierlei: Mit dem Gewaltmonopol erhält der Staat die Aufgabe, das „Eigentum" der Bürger zu schützen. Zu ‚treuen Händen' erlangt dieser so die (ausschließliche) Möglichkeit, eine individuelle gewaltsame Rechtsdurchsetzung zu kontrollieren und zu sanktionieren und damit Sicherheit (im gesellschaftlichen Gefüge) herzustellen (dazu auch Hartmann 2011). Für den Bürger ist dieses

„Anvertrauen“ von natürlichen Rechten jedoch auch riskant, denn, folgt man der Lesart Baiers (2001) und Hartmanns (2011: 446ff., 2013), umfasst das anvertraute Eigentum nicht nur materielle Besitzstände, sondern darunter ist auch der Schutz des Lebens zu verstehen. Im Gesellschaftsvertrag verwirklichen sollen sich auch die individuellen Freiheitsrechte, wie z.B. die Bewegungs- oder Meinungsfreiheit (ebd.: 622):

> „Obwohl die Erde und die niedrigeren Geschöpfe den Menschen gemeinsam gehören, so hat doch jeder Mensch ein Eigentum an seiner eigenen *Person*; auf sie hat niemand ein Recht als nur er allein. Die *Arbeit* seines Körpers und das *Werk* seiner Hände sind, so können wir sagen, im eigentlichen Sinne sein Eigentum.“ (Locke 1977: 216, Herv. i.O.)[70]

Eine vertrauensvolle Übertragung von Kontrolloptionen geht deshalb zugleich mit einem Misstrauen gegenüber der mit dieser Macht verbundenen Potenzen einher, sind doch, so die Moralphilosophin Annette Baier (2001: 45), diejenigen, denen wir vertrauen, um die uns wichtigen Dinge zu erschaffen und zu erhalten, jene, denen eine Verletzung am leichtesten fiele. So bezieht sich der Begriff im Besonderen darauf, einem Gegenüber die Ausführung einer Angelegenheit, sei sie allein erschaffbar oder nur mit Hilfe anderer zu erhalten, vertrauensvoll zu übertragen. Wie bereits in Kapitel 3.2.2.2 ausgeführt, ergibt sich die Relevanz des Vertrauens also vor allem aus seiner Einbettung in Verhältnisse zu Anderen, über deren Motive für und über deren zukünftiges Handeln selbst keine ausreichenden Informationen vorhanden sein können. Im Vertrauen zeigt man sich zuversichtlich, dass dieser die Verletzungsgelegenheit – eine Freiheit des Handelns, die das Vertrauen gerade erst erforderlich werden lässt – nicht nutzen wird (Baier 2001: 43). Verwiesen ist dann auch auf die Grenzen eines Bedürfnisses nach Wissen und einen durch das „institutionalisierte Misstrauen“ definierten „Ermessensspielraum“ (ebd.: 46ff.). Bei Locke ist es ein moralisches Moment (Hartmann 2002: 386) des Vertrauens, das sich im Verhältnis zwischen Bürger und Staat etabliert. Die Legislative ist

> „eine Gewalt, die auf Vertrauen beruht und zu bestimmten Zwecken handelt. Es verbleibt dem *Volk* dennoch die höchste Gewalt, die Legislative abzuberufen oder *zu ändern*, wenn es der Ansicht ist, daß die *Legislative* dem in sie gesetzten Vertrauen zuwiderhandelt.“ (Locke 1977: 293f., Herv. i.O.)

Für Hartmann (2002: 393) besteht nun ein wesentlicher Unterschied zu modernen politischen Verhältnissen darin, dass die Bürger zum misstrauischen Inspizieren der Vertrauenswürdigkeit angehalten sind und sich nicht auf die Moralität des Handelns verlassen. Für demokratische Gesellschaften gilt dann auch ein paradox anmutendes Verhältnis von Vertrauen und

[70] Anders als im Naturzustand ist, Lockes (1977: 200ff.) Überlegungen nach, im Gesellschaftsvertrag der Zustand vollkommener Freiheit und Gleichheit zwar aufgehoben, gleichsam aber nur so zu erhalten, um die Unsicherheiten, die aus dem freien Handeln anderer Personen, die den eigenen Besitz an Leben, Freiheit, Gesundheit und Besitz gefährden könnten, zu reglementieren.

Kontrolle in Form institutionalisierten Misstrauens gar als konstitutiv, wie Piotr Sztompka (1998) herausgearbeitet hat. So ist Vertrauen als Ausdruck staatlichen Handelns vor das Problem gestellt, dass Institutionen ihre Vertrauenswürdigkeit unter Beweis stellen müssen, selbst jedoch nicht vertrauen können. Um Sicherheit und Freiheit gleichermaßen zu gewährleisten, sind in demokratischen Kulturen dem „Ermessensspielraum" (Baier 2001: 46ff.) staatlichen Handelns, in Form „institutionalisierten Misstrauens" (Sztompka 1998: 26), Grenzen gesetzt, die die Reichweite fürsorglicher staatlicher Kontrolle bestimmen: Regelmäßige Wahlen und überschaubare Legislaturperioden garantieren nicht nur die Legitimität staatlicher Macht. Das Prinzip der Gewaltenteilung, eine unabhängige Justiz und unabhängige Medien, die verfassungsmäßige Regierung und Rechtsstaatlichkeit sind durch die Verfassung etablierte Mechanismen, welche die rechtsetzenden und rechtsdurchsetzenden Institutionen selbst der Kontrolle unterziehen. Im gegenseitigen Verweis aufeinander bestimmen sie sowohl den staatlichen als auch den zivilgesellschaftlichen Freiheitsraum des Handelns. Ein „Gefühl" der Rechtmäßigkeit und existentieller Sicherheit – in Sztompkas (ebd.: 23) Worten: „a feeling of orderliness, predictability, regularity and existential security" –, das vom „Risiko der Vertrauensgewähr" (Luhmann 2000: 4) entlastet, ist durch diese Prinzipien und Mechanismen – z.B. in Gestalt verbürgter Grundrechte oder indem die Gesetze hinreichend eindeutig und konsistent sind und ihre Anwendung berechenbar ist – gewährleistet. Diese institutionalisierten Kontrollmechanismen ermöglichen dort, wo sie etabliert werden, den Verzicht auf weitere Kontrollerfordernisse, sodass sich (personales und institutionelles) Vertrauen als kulturelle Ressource etablieren kann. Die Etablierung einer solch normativen Gewissheit ist die Voraussetzung für eine Freiheit des Handelns auf beiden Seiten. Der Wert des Vertrauens ist insofern normativ inspiriert (Hartmann 2007: 6). Im Verzicht auf Kontrolle kann es sich der Notwendigkeit vollständigen Wissens entledigen. Im Hinblick auf das vorgängige Vertrauen als Bedingung von Akzeptanz, wie es in Kapitel 3.2.2.2 dargestellt wurde, zeigt sich, dass die Kontrollmechanismen ihre Stärke aber gerade daraus zu ziehen, dass sie eher im Hintergrund bleiben (Sztompka 1998: 29).

Im vertrauensvollen Handeln entfaltet sich eine Form des Engagements (Hartmann 2011: 58), das weniger darauf abstellt, aktiv Zeichen für Vertrauenswürdigkeit zu suchen, sondern sich gerade im Kontrollverzicht und darüber hinaus darin ausdrückt, dass Zeichen, die misstrauisch stimmen könnten, fehlen. Während sich Vertrauen also „nicht auf Beweisen, sondern auf einem Mangel an *Gegenbeweisen* gründet" (Gambetta 2001: 235, Herv. i.O.), etabliert sich Misstrauen gerade vor dem Hintergrund von wenigen, gleichwohl überzogenen Informationen (Luhmann 2000: 93) bzw. Anzeichen und Unstimmigkeiten einer nun fragwürdig gewordenen

Vertrautheit. Bildet Vertrautheit eine Voraussetzung für Vertrauen, zieht es denn auch nicht notwendigerweise Vertrauen nach sich. Sowohl Vertrauen als auch Misstrauen können auf Vertrautheit folgen (Luhmann 2000: 94f.).

Aus einer soziologischen Perspektive sind Vertrauen und Misstrauen zunächst weder gut oder schlecht (Endreß 2012: 86, Lewicki et al. 1998). Als ein „funktionales Äquivalent“ zum Vertrauen (Luhmann 2000: 92) leistet Misstrauen in gleichem Maße Vereinfachung, das heißt es reduziert Komplexität, ohne dabei auf eine Haltung begrenzt zu sein (ebd.: 94). Es handelt sich dabei vielmehr um normative Zurechnungen (Endreß 2012: 86), die ebenso historisch variabel sind, wie die Perspektiven darauf, welches Maß an Vertrauen oder Misstrauen als ‚angemessen‘ bzw. als problematisch zu bewerten ist. Wie Luhmann (2000: 94) betont wäre es bereits eine Übergeneralisierung anzunehmen, dass jemand „nur Gutes oder nur Schlimmes erwarten (könne).“ Vielmehr und darauf weist dann auch Endreß (2012: 88 mit Bezug auf Lahno 2002: 215f.) hin, wird die Wirklichkeit eher als ambivalent, das heißt vor dem Hintergrund potentiellen Vertrauens und Misstrauens erlebt. Das insofern vorzunehmende Ambivalenzmanagement zeichnet sich, bildlich gesprochen, als der „alltägliche Balanceakt zwischen fraglos Hingenommenem, bereits fragwürdig Gewordenem und prinzipieller potentieller Fragwürdigkeit“ (Endreß 2012: 88) aus. Ist mit der dialektischen Beziehung von Vertrauen und Misstrauen (Sztompka 1998: 290) auf die Grenzen des Wissbaren in komplexen Gesellschaften verwiesen, werden mit den jeweils verfügbaren und eingesetzten ‚token of trust‘ wie biometrischen Verfahren, die darauf zielen Wissen zu generieren, zugleich Grenzen des Vertrauens virulent. So steht das Begehren nach Wissen dem Vertrauen, sowohl im Verhältnis zur Gegenwart als auch Zukunft prinzipiell konträr entgegen. Die Fragen nach dem Verhältnis von Vertrauen und Misstrauen im Hinblick auf die Nutzung von Biometrie sind dabei auf unterschiedlichen Ebenen verortet. Die alltägliche Verbreitung von Technologien wie des Fingerabdruckverfahrens wird, erstens, dahingehend problematisiert, dass Sicherheitsbereiche zunehmend ausgeweitet werden (vgl. z.B. Ceyhan 2008). Im Hinblick auf die Funktionsweise der biometrischen Verfahren deutet sich eine Ausweitung des Sicherheitsimperativs an: „constantly seeking to establish its markers of certainty and fixity“ (ebd.: 1), indem, technologisch mediiert, alles nur Mögliche interpretiert wird (Lodge 2013: 313). Der Einsatz des Verfahrens, etwa in seinem staatlichen Anwendungsbereich, lässt sich so als ein Versuch verstehen, sich mit dem „Unvertrauten“ vertraut zu machen, indem die Technologie Wissen generieren soll und mithin Misstrauen transportiert. Luhmann folgend verstehen etwa Lewicki et al. (2008: 446) Misstrauen als Ausdruck von „wariness, skepticism, and such behavior as observed defensiveness, watchfulness, and vigilance“, das seinen Ausdruck in Überwachungs-

praktiken oder institutionalisierten Kontrollen findet. Angesichts einer „Normalität von Unsicherheit“ soll die „Übersetzung“ körperlicher Merkmale und Eigenschaften ein Mehr an Informationssicherheit erbringen (Aas 2006: 144). Juliet Lodge (2013), die die Rolle der Biometrie für die Umsetzung von (Un-)Sicherheit und Überwachung untersucht und die bereits in Kapitel 1.1.2.2 skizzierten Risiken rekapituliert, entdeckt in der vorausgesetzten Logik ihrer Verwendung dann auch ein über-optimistisches und unberechtigtes Vertrauen in ihre Funktionsfähigkeit – wie es sich im Übrigen in der vorliegenden Studie im Hinblick auf die unbefragte Funktionalitätsunterstellung zeigte (vgl. Kapitel 3.1.3). Zweitens verringere sich Vertrauen in dem Maße, wie mit der Verbreitung automatisierter Kontrolle, im Besonderen biometrischer Technologien, das Vertrauen in Technik personalisiertes Vertrauen ablöse. So werden aus der Arbeits- und Funktionsweise biometrischer Techniken weitreichende Konsequenzen für Grundprinzipien des Sozialen abgeleitet, denn wie sich Menschen identifizieren zeige, so Aas (2006: 144ff.), auch, wie sie Vertrauen etablierten, weil, in anderen Worten, mit Biometrie nicht länger Vertrauen in den kooperativen Nutzer gesetzt werden muss.

In gleichem Maße, wie die Technologie dazu dienen soll, Sicherheit herzustellen, können damit einhergehende Wissens- und Kontrollambitionen, drittens, Verunsicherung und Misstrauen erzeugen und, etwa als Ausdruck ungerechtfertigter Kontrolle, Vertrauen unterminieren (z.B. Ellis 2011) oder gar Misstrauen generieren. Ein Verlust von Vertrauen oder gar die Entstehung von Misstrauen kann sich dadurch realisieren, dass Sicherheitsmaßnahmen als Zwangsmaßnahmen wahrgenommen werden. Hängt die Leistungsfähigkeit abstrakter Systeme auch davon ab, in welcher Weise sie selbst Vertrauensbeziehungen herzustellen vermögen – setzt doch Vertrauen als Verhältnis, das sich um ein „anvertrautes“ Gut etabliert, die Kooperation gerade voraus, nämlich dass auch derjenige, dem vertraut wird, sich auf die Vertrauenswürdigkeit und Kompetenz des Vertrauensgebers verlässt (vgl. Hartmann 2011: 240ff.; Baier 2001) –, dann kann auch eine „Schwelle“ des Handelns (Luhmann 2000: 37) erreicht sein, die das Vertrauen in den Staat und seine Institutionen bedroht, wenn das Handeln von Sicherheitsbehörden als nicht mehr zurechenbar, als intransparent oder willkürlich wahrgenommen wird.

3.3.3 Grenzen des Vertrauens

Die Grenzen des Vertrauens etablieren sich für die Befragten entlang von zwei idealtypischen Dilemmata. So nehmen sie, erstens, die Technologie als Ausdruck eines grundsätzlichen Misstrauens gegenüber der Bevölkerung wahr und kritisieren in diesem Zusammenhang die

Unbegrenztheit des staatlichen Sicherheitsbedürfnisses, das sich in einem Gefühl ubiquitären Verdachts äußert. Zweitens lässt sich eine ambivalente Haltung gegenüber staatlichen Handelns ausmachen, die sich vor allem aus der Nicht-Zurechenbarkeit möglicher Handlungsintentionen generiert.

3.3.3.1 Biometrie als Ausdruck von Misstrauen

Luhmann (2000: 92ff.) zufolge ist Misstrauen durch negative Erwartungen geleitet, oder wie es Patti Tamara Lenard (2008: 316) formuliert, „reflects suspicion or cynicism about the actions of others." Zieht eine solche Haltung eher abwehrendes denn gemeinschaftliches Handeln nach sich, dann zeigt sich zunächst, dass – im Übrigen auch allein aus theoretischen Überlegungen heraus, das heißt, wenn Befragte das Verfahren eigentlich in anderen Zusammenhängen nutzten –, Akzeptanzvorbehalte daher rühren, weil die Aufforderung zur Fingerabdruckabgabe als ein institutionalisiertes Misstrauen des Staates gegenüber seinen Bürgern gedeutet wird. Stellvertretend für andere Befragte bedauert etwa die 19-jährige Schülerin Simone Kutzer (Schul1) die ausdrückliche Misstrauenserklärung des Staates an seine Bürger durch die Einführung der Fingerabdrücke in die Ausweisdokumente:

> „Also da find ich das jetzt nich' so gut. ((lacht)) Mm, ja einfach weil ich find das Vertrauen zu den B-, also, ja, dass der Staat nich' genug Vertrauen zu seinen Bürgern hat, find ich schon schade, also, ich weiß nich' ob der Staat denkt, dass alle kriminell sind oder Terroristen oder was weiß ich ((lacht)). Find ich schon extrem, dass diese Welle seit dem 11. September eben so übertrieben is'. Ja, also ich find es nich' so schön."

Diese Einschätzung korrespondiert mit Einschätzungen im öffentlichen Diskurses, wonach die seit 2001 eingeführten Sicherheitsmaßnahmen Gefahr laufen, das Vertrauensverhältnis des Staates zu seinen Bürgern zu verspielen. Diese werden als Umkehr des Prinzips der „Institutionalisierung von Misstrauen" gedeutet, und dahingehend kritisiert, dass sie den Bürger so unter einen Generalverdacht stellen (z.B. Prantl 2002, Gössner 2002). Als unangemessenen Ausdruck von Misstrauen deuten dann auch Antragsteller von Ausweispapieren die Fingerabdrucktechnologien. Wie in Kapitel 3.2.1.3 ausgeführt, werden sowohl von Befürwortern als auch expliziten Ablehnern der Fingerabdrucktechnologie im behördlichen Kontext die Mitarbeiter zwar für Misstrauensbekundungen immunisiert, weil an ihnen selbst nichts *„auszusetzen"* ist (Louise Petersen, Einwo). Problematisiert wird in diesem Zusammenhang vielmehr eine fehlende Transparenz und Partizipation bei der Entscheidungsfindung, wie Sicherheit herzustellen ist – das Ehepaar Petersen (Einwo) als ausdrückliche Ablehner, ebenso das Ehepaar Oppermann (Einwo) als ambivalente Annehmer der Technologie gleichermaßen monieren den

Zwang zur Fingerabdruckgabe für die Ausstellung eines Reisepasses. Hier buchstabiert sich die Problematisierung entlang des von Sztompka (1998: 23ff.) entwickelten Modell vertrauensbegründender Bedingungen demokratischer Rechtsstaatlichkeit aus, in der der Vertrauensbruch zunächst darin liegt, „dass die Bürger am Prozess der genauen Abstimmung von Sicherheits- und Freiheitsbedürfnissen nicht wirklich beteiligt werden“ (Hartmann 2012: 622). Darüber hinaus wird die Abfrage dieser neuen Informationen selbst für einige Befragte zum Symptom für ein fehlendes Vertrauen, mithin ausdrückliches Misstrauen des Staates gegenüber seinen Bürgern. Ausgehend von einer ausdrücklichen Kritik daran, nicht hinreichend auf die Verpflichtung zur Fingerabdruckabgabe hingewiesen worden zu sein, eruiert Frau Petersen, woran sich wohl die Indizien von Gefahr, auf die die Fingerabdruckgabe vermeintlich zielt, an ihrer Person ausmachen ließen:

> Alfons Petersen: „Ne! Oder bei dir, stand auch nix, wenn man noch ‘ne andere Staatsangehörigkeit hat, dass man dann noch besondere Formulare ausfüllen muss.“
>
> Louise Petersen: „Jaaaa, du, ich hab‘ Verständnis, weil“
>
> Alfons Petersen ((fällt ins Wort)): „Man sollte da drauf vorbereitet sein. Vielleicht sagt man‘s mal so, ne?“
>
> Louise Petersen: „Die Welt hat sich geändert. Also, was alles passiert und französisch sprechende Länder und was da alles passiert, ich kann es mir gut vorstellen, dass sie, dass sie jetzt so fragen, nich‘? Nur, ich gehör doch auch dazu ((hebt die Stimme)), das is‘ es, ne? (Herr Petersen brummt zustimmend, I: „Ja ja“). Ich, man muss sich identifizieren, nich‘? Mh? Ja, ich hab‘ eine andere Staatsangehörigkeit, ich komm aus einem anderen Land, ich könnte auch alles Mögliche machen, ja, sagen wir, ne? Deswegen. Gut, is’ in Ordnung.“

Im Hinblick auf die Antragssituation erlebt vor allem Frau Petersen ein „Unvertrautwerden“ (vgl. Luhmann 2000: 22ff.) mit der Welt. Dass sich offenbar die Zurechenbarkeiten staatlichen Handelns verändern, geht für sie mit starken emotionalen Erfahrungen einher (vgl. auch Kapitel 3.2.1.3). Die Offenlegung und Kontrolle von Fremdheit erscheint für Frau Petersen die zentrale Intention der Fingerabdruckgabe, sodass sie die Situation in der Einwohnermeldebehörde dann auch als Prozedur erlebt, weil daraus ein spezifisches Misstrauen ihr selbst gegenüber zum Ausdruck kommt, das zudem ein Exklusionsempfinden auslöst. Die Notwendigkeit einen Fragebogen zur Staatsangehörigkeit auszufüllen und die Aufforderung zur Fingerabdruckabgabe erscheinen ihr als Degradierungspraktik, die sie, ungerechterweise, als Nicht-Teilhabeberechtigte ausweisen. Während sie versucht, die Kontrollprozedur im Verhältnis zu einer allgemeinen Bedrohungslage, die ein Misstrauen gegenüber allem Fremden erklärt, sowie die grundsätzliche Verpflichtung zur Identifikation zu relativieren, bleibt gleichwohl das Gefühl ungerecht behandelt worden zu sein, denn: *„Ich gehör doch auch dazu“*. Die

im Interview formulierten Akzeptanzvorbehalte lassen sich, ausgehend von der „relational perspective on authority“ (Tyler/Lind 1992) damit erklären, dass Compliance, zum einen, auch von der Wahrnehmung davon abhängt, wie die eigene Vertrauenswürdigkeit durch staatliche Autoritäten vermittelt wird. Ein fehlender Respekt, der sich so Tom R. Tyler (1998: 281ff. mit Bezug auf Tyler/Degoey/Smith 1996) in solcherart Identitätsurteilen ausdrückt, beeinflusst auch die Beurteilung der Legitimität staatlichen Handelns. Denn wie vor allem Tyler (1998) zudem herausgestellt hat, folgen Bürger den Entscheidungen der Regierung und staatlicher Entscheidungen nicht aufgrund von Sanktionsdrohungen, sondern aufgrund des Glaubens, dass diese prinzipiell in ihrem Interesse bzw. zu ihrem Wohl handeln. Fragebogen und Fingerabdruckverfahren sind jedoch sich aus der Vertrautheit der Behördensituation hervorhebende Unstimmigkeiten und für Herrn Petersen Anlass für ein ausdrückliches Misstrauensurteil gegenüber dem Staat. So stellt er die wohlwollende Intention des Staates selbst in Frage – *„Was bringt das? Können Sie [die Interviewerin] mir eine Antwort geben?“* – und in Bezug auf die Technisierung von Kontrolle, wie sie sich im Fingerabdruckverfahren ausdrückt, in den Kontext einer Entwicklung zu einem autoritären Staatswesen, dass darauf ist *„noch mehr Einfluss“* auf seine Bürger zu nehmen:

> Alfons Petersen: „Kennen Sie das Buch ‚1984‘?“
>
> I: „Natürlich.“
>
> Alfons Petersen: „Natürlich, ne? ((alle lachen leicht)) Seh‘n Sie, als ich noch zur Schule ging, haben wir über das Buch auch diskutiert und haben gesagt, das wird nie möglich sein. Dass man so was schafft wie dieses System, und das war ja noch einfach im Vergleich zu dem, was wir jetzt haben. Ja? Das is‘ also ein Fortschritt in Tüdelchen.“

Während für viele Befragte die Dystopie in der zukünftigen Möglichkeit real ist, qualifiziert die Verfügung über fortgeschrittene Kontrolltechnik für Herrn Petersen einen nicht mal im Literarischen hinreichend imaginierten *„Fortschritt“* und für ihn per se eine explizite Vertrauensschwelle, die seine von ihm selbst als *„misstrauisch“* beschriebene Grundhaltung verstärkt. Soll die biometrische Technologie, auf der einen Seite, Sicherheit garantieren, mithin das Sicherheitsgefühl steigern, erzeugt eine sich darin ausdrückende staatliche Kontrollambition, auf der anderen Seite, potentiell auch ein Gefühl der Verunsicherung, weil der Verdacht ubiquitär und nicht mehr nachvollziehbar wird (Hartmann 2013: 624). Während die spezifische Sicherheit des Vertrauens mit Luhmann (2000: 9) darin liegt, dass ich mich darauf verlassen kann, dass die Konditionen, unter den ich heute handle, ebenso wie die Konsequenzen, die dieses Handeln mit sich bringt, auch morgen noch die gleichen sein werden wie gegenwärtig, kann eine diffuse Allgegenwärtigkeit von Kontrolltechnologien das Vertrauen in die

eigenen Erwartungen und die eigene Handlungssicherheit erschüttern. Wenn morgen schon alles zum Risiko werden kann, worauf könne man sich dann noch verlassen, woran das Handeln ausrichten? Angesichts eines solchen „Unvertrautwerdens“ mit der Welt (vgl. Luhmann 2000: 22ff.) gerät dann auch das eigene Handeln zum Risiko. Der 25-jährige Stephan Löw (Einwo) lehnt dann auch ausdrücklich die Speicherung der Fingerabdrücke in den Personalausweis nicht nur deshalb ab, weil sich für ihn die Fingerabdruckgabe aufgrund der polizeilichen Assoziation nur im Rahmen einer Verdachtsgewinnung legitimiert. Er weist zudem das Sicherheitsargument als *„fadenscheinig“* aus und unterstellt der behördlichen Argumentation eine Täuschungsabsicht dahingehend, dass im Alltag etwa in Polizeikontrollen eine Überprüfung der Fingerabdrücke zur Identitätsfeststellung unwahrscheinlich sei. Demgegenüber sei aufgrund der Eindeutigkeit des *„Codes“* Fingerabdruck dieser jedoch geeignet, eine eindeutige Kontrolle und ungerechtfertigte staatliche Überwachung zu ermöglichen:

> Stephan Löw: „Und das, das is‘, womit man jemanden auch über ‘n relativ langen Zeitraum immer wieder identifizieren kann. Ich denke, damit hat es was zu tun, dass es alles so wirklich diese Überwachung des Bürgers gut möglich is‘.
>
> I: „Sollte das auch so sein, oder würden Sie sagen, das sollte nich‘, sollte nich‘ so sein?“
>
> Stephan Löw: „Nein. Das sollte nich‘ so sein.“
>
> I: „Warum? Können Sie das näher beschreiben?“
>
> Stephan Löw: „Weil ich der Meinung bin, dass es eigentlich Sache des Bürgers ist, selbst über seine Daten mit entscheiden zu können und dass der Staat sich in gewissen Dingen nicht einzumischen braucht.“

Die kritische Betroffenheit, die Herrn Löw zur Verweigerung der Fingerabdruckspeicherung motiviert, drückt sich also nicht nur darin aus, dass er sich unberechtigt verdächtigt fühlt, sondern auch in einem Unbehagen, in seiner eigenen Freiheit eingeschränkt zu werden und damit die Möglichkeit wahrnehmen zu können, diese fernab der Erwartungen Anderer entfalten zu können, das heißt nicht gegen den eigenen Willen gekannt zu werden. Denn dieser „Kernbestand menschlicher Würde und Autonomie“ (Ammicht-Quinn/Rampp 2009: 146) in Freiheit handeln zu können, erscheint durch Überwachungsmöglichkeiten dann zumindest eingeschränkt, wenn sie die ständige Auseinandersetzung mit Normalitätsanforderungen (Endreß/Rampp 2013: 150) bzw. Aufforderungen zur Unschuldsversicherung (vgl. Hartmann 2013: 824) bedeuten. In dieser Passage drücken sich dann, wie bereits in Kapitel 3.2.2.1 skizziert, Vorstellungen von Privatheitsbereichen, die durch das spezifische Verhältnis von Datenpreisgeber und -nehmer etabliert werden, aus. Ausdrücklich fordert Herr Löw dann auch ein Recht auf informationelle Selbstbestimmung ein und dies, wie er dann weiter ausführt, vor allem vor dem Hintergrund der vermuteten riskanten Datenverwendung:

> Stephan Löw: „So, ich sollte Herr meiner Daten sein. Und, wem ich die geben möchte, dem kann ich sie geben, und, und ich weiß halt nich‘, was so im Hintergrund von Unternehmen oder im Hintergrund von staatlichen Stellen oder so, was da mit der Amtshilfe oder so läuft. Mit meiner Adresse jetzt. Oder wo, wenn ich irgendwohin fliege oder so, an welche Staaten dann übermittelt wird, in welchem Flug ich grade fliege, und denn quasi gleich der gesamte Datensatz mit rüber wandert. Und nich‘ nur der Name, sondern auch die Adresse, meine Körpergröße und gleich die biometrischen Daten gleich mit. So.“

Ebenso wie das Vertrauen, kann sich also das Misstrauen in den kontextuell etablierten Regeln der Datenverwendung gründen, denen gegenüber sich Herr Löw vor dem Hintergrund der Freiwilligkeit der Datenpreisgabe sensibel zeigt. Die Ungewissheit über die Datenverwendung lässt dann auch für Befragte das in staatliches Handeln gesetzte Vertrauen ambivalent werden.

3.3.3.2 Ambivalentes Vertrauen: Die Unzurechenbarkeit staatlichen Handelns

Für einige Befragte geht mit der Preisgabe der Fingerabdrücke zwar kein generelles Misstrauen, sondern vielmehr eine Irritation des Vertrauens einher, die vor allem darin gründet, dass die wahrgenommenen staatlichen Sicherheitsambitionen auch die gesetzlichen Grenzen staatlichen Handelns tangieren könnten. So entscheidet sich Herr Zander (Einwo) zwar für die Aufnahme des Fingerabdrucks in seinen neuen Personalausweis und verweist hinsichtlich des von ihm wahrgenommenen, zumindest theoretischen, Nutzens auf die legitime Kontrolle seiner Identität durch die Polizei. Die unberechtigte Weitergabe und Verwendung seines Fingerabdrucks durch staatliche Behörden hält Herr Zander angesichts der allgegenwärtigen Sammlung von nebenher preisgegebenen Daten gleichwohl für durchaus möglich:

> „Bei der derzeitigen Sicherheitslage des Staates ist es für mich natürlich grad interessant, wer wo wann war. […] Also im Falles eines Falles wird so ein Abgleich sicherlich gemacht. Ob jetzt, ob jetzt da der Richter zustimmen muss oder nich‘, das is‘ sehr fraglich, aber wenn das, ich sag‘ mal, wenn das technisch möglich is‘, wird es auch gemacht.“ (Christian Zander, Einwo)

Herr Zander formuliert in dieser Passage dann auch ein Unbehagen darüber, dass das, was technisch möglich ist, auch getan wird, weshalb dann auch sein Vertrauen in das im Recht verankerte staatliche Handeln fraglich wird, weil hier die „Funktionsfähigkeit [der] immanenten Kontrollen“ (Luhmann 2000: 77) in Frage gestellt wird. Die Eigenmächtigkeit staatlicher Sicherheitsagenturen, sich über gesetzliche Grenzen hinwegzusetzen, hält ein anderer Befragter sogar für hochgradig wahrscheinlich. Befragt nach seinen Vorstellungen über die Verwendung seines Fingerabdrucks im ePass erklärt er:

> „Gut. Ich denk mal so, eine Geschichte ist erstmal klar, die Bundesdruckerei wird das nicht speichern, aber ich unterstell‘ dem deutschen Geheimdienst jetzt einfach mal so, dass er mit Sicherheit diesen Fingerabdruck gespeichert wird, weil es sind sehr nützliche Informationen, und sie nicht zu verwerten wäre sowas, ich sag mal, Militär, und vom MAD oder BND, einfach mal nicht sehr klug.“ (Carsten Welzer, Einwo)

Beide Befragte sind zwar darum bemüht, die eigentlich nicht tolerierbaren Folgen der Datenpreisgabe zumindest dort, wo es ihnen möglich erscheint, zu vermeiden: also etwa nicht mit der Kreditkarte, sondern bar zu bezahlen (Christian Zander, Einwo) oder bei facebook die preisgegebenen Daten zu *„beschränken“* (Carsten Welzer, Einwo). Beispiele wie die *„Handy-Vorratsdatenspeicherung“* (Christian Zander, Einwo) oder die Aufhebung des *„Bankgeheimnisses“* (Carsten Welzer, Einwo) zeugen aber gleichwohl von der Allgegenwart und Unumkehrbarkeit potentieller Überwachung. *„Dieses Überwachen, Kontrollieren, Speichern, das ist nicht mehr revidierbar“*, so Herr Zander, stellvertretend auch für Herrn Welzer, unabhängig davon, wer ausspäht: der Staat oder *„jeder Hacker“*, oder was ausgeleuchtet wird: Handydaten oder Internetsuchverläufe. Und so betont er in Anspielung auf die rhetorische Figur des „gläsernen Bürgers“ aus dem kritischen Diskurs zu Überwachung:

> „Gläsern ist man ja nicht, man ist sichtbar. Du bist ja soweit du irgendwo bezahlst erscheint ja irgendwo deine, deine EC-Kartennummer oder dein Name oder, oder. Ich sag‘ dazu Datensätze. Sag’ ich mal dazu. Was mit den Datensätzen passiert, weißt du im Moment der Abgabe nicht.“

Wenn die Verfügbarkeit über Kontroll- und Überwachungstechnologien mit staatlichen Sicherheitsambitionen verknüpft wird, die tendenziell neue Sichtbarkeitsregime erschaffen und so auch Erwartungssicherheiten in das Recht erschüttern, dann zeigt sich gleichwohl, dass diese Irritationen nicht zwangsläufig in Misstrauen umschlagen. Der potentielle, das heißt vorstellbare, Missbrauch der Daten findet etwa für Herrn Zander seine Grenzen im staatlichen Sicherheitsstreben selbst und so zeigt er sich zuversichtlich, dass der staatliche Datenaustausch etwa mit der Gebühreneinzugszentrale (GEZ), mithin zu *„privaten Zwecken“*, nicht realisiert wird. Ein Vertrauen in das von Sicherheit geleitete Handeln des Staates zeigt sich hier als ausschlagend dafür, dass, anders als etwa bei Ehepaar Petersen, die eine explizite Staatsskepsis formulieren, die Ambivalenz des Vertrauens nicht in ausdrücklichem Misstrauen mündet. Auch die Möglichkeit des Missbrauchs, wie sie Herr Welzer für wahrscheinlich hält, vermag das Vertrauen in den Staat nicht grundsätzlich zu erschüttern, denn ausdrücklich vertraut er diesem und formuliert demgegenüber Vorbehalte gegenüber *„einzelnen Menschen.“*

3.3.4 Zusammenfassende Überlegungen

Die Ambivalenz des Vertrauens (Möllering 2006: 6; Endreß 2008) verweist auf die Bedingungen von Vertrauensverhältnissen. So bedeutet zu vertrauen keineswegs den Verzicht auf jegliche Information oder, in Anette Baiers (2001: 43) Worten, auf „gute Gründe". Vertrauen ist demnach nicht naiv, sondern der Spielraum, der sich im Vertrauen eröffnet und von Kontrolle entlastet, besitzt Grenzen. Auch Martin Endreß (2001: 170f.) betont, dass Vertrauensverhältnisse nicht als Abhängigkeitsverhältnisses, die aus blinder Zutraulichkeit entstehen, zu verstehen sind. Vielmehr etablieren sich die Grenzen des Vertrauens aus der Reichweite reziproker Handlungserwartungen im Rahmen der durch das Vertrauen ermöglichten Freiheitsräume (vgl. Gambetta 2001), oder in Annette Baiers Worten (2001: 46):

> „Wenn man uns vertraut, verlässt man sich darauf, dass wir uns genau um die Sache kümmern, über die man uns ein wenig verfügende Verantwortung eingeräumt hat, und tatsächlich ist es so, dass normale Personen die Hinweise aufnehmen, die die Grenzen dessen anzeigen, was ihnen anvertraut worden ist".

Wo, wann und auf welcher Basis diese gezogen werden, ist dann, wie etwa Annette Baier aus dem Modell des *An*vertrauens von John Locke folgert, wiederum eine Frage des jeweils zu betrachtenden Vertrauensverhältnisses und damit auch der in Frage stehenden legitimen Zwecke und der Vorstellungen von den etablierten Regeln der Datenverwendung. Auch nach Martin Hartmann (2011) lassen sich diese nur an der Vertrauenspraxis selbst bemessen. Vertrauen, ebenso wie Misstrauen, lassen sich dann, analog zur Akzeptanz, als eine dreistellige Relation verstehen. Das Vertrauen wird durch eine Schwelle kontrolliert, bevor es in Misstrauen umschlägt: Als Bedingung für ein solches Umschlagen lässt sich die Technologie selbst ausmachen, die als Indiz für fehlendes staatliches Wollwollen und mitunter auch schädigende Absichten interpretiert wird. Gleichwohl erweisen sich Vertrauen und Misstrauen nicht als gegensätzliche Enden auf einem Spektrum, sondern sind vielmehr teils koexistierende Haltungen und Bestandteil des alltäglichen Ambivalenzmanagements (Endreß 2012: 88), das mit dem Akzeptanzhandeln einhergehen kann. Oft genug finden sich die Befragten in einem Zustand wider, in dem sie mit sich widersprechenden Einschätzungen ringen und die sich als kritische Eingabe in staatliche Sicherheitsambitionen lesen lassen. Eine allgemeine Misstrauenskultur, wie es die Surveillance Studies argwöhnen, zeichnet sich vor dem Hintergrund der Ergebnisse der Studie zwar nicht ab. Die emotionale Involviertheit von Frau Petersen aufgrund des ausdrücklich angenommenen Misstrauen führt jedoch zu der Frage nach dem Effekt institutionellen Misstrauens, wie es etwa Darren Ellis (2011) zu Erfahrungen „ontologischer Unsicherheit" (ebd.: 5) untersucht hat. Er bezieht sich u.a. auf eine Studie von Greg Noble (2005, „The Discomfort of Strangers: Racism, Incivility and Ontological Security in a Rela-

xed and Comfortable Nation") und beschäftigt sich mit den Erfahrungen „ontologischer Unsicherheit" (ebd.: 5) von v.a. islamischen Migranten in Australien nach den Ereignissen am 11. September 2001. Danach seien Islamophobie und ihr Widerhall in politischen Diskursen Ausdruck institutionalisierten Misstrauens. Für die von dieser kontinuierlichen Erfahrung betroffenen Bürger seien damit tiefe emotionale Einflüsse verbunden, die sich auf die Fähigkeit, personelles Vertrauen aufzubauen, auswirkten (ebd.: 9). Ein Vertrauensverlust kann auch weitreichende Konsequenzen für eine demokratische Kultur haben. Wie Benjamin Goold (2009: 208ff.) mit Blick auf den umfangreichen Einsatz von Videokameras in Großbritannien problematisiert, riskiert der undifferenzierte Einsatz von Überwachungstechnologien einen Vertrauensverlust der Bürger in den Staat und mit ihm eine zumindest minimale Unterstützung in die Regierung. In der Folge, so fürchtet Goold (ebd.: 207), könne dies eine Hinwendung zu alternativen, nicht demokratischen Regierungsformen nach sich ziehen: „The increasing trend towards greater levels of state surveillance has the potential to undermine well-established norms of governance based on consent and shared commitment to democratic forms of government."

4 Schluss

Angesichts einer zunehmenden gesellschaftlichen Bedeutung freiwillig oder kooperativ preisgegebener Daten im Alltagsleben wird regelmäßig die Frage nach den Bedingungen dieser neuen Bereitwilligkeit aufgeworfen. Diese ist vor allem von einem Unbehagen darüber getrieben, das sich, zum einen, daran festmachen lässt, dass diese Datenpreisgabe bedeutet, sich potentiell erweiterten Kontrollbefugnissen zu unterwerfen – könnten doch verschiedenste Akteure über die preisgegebenen Daten verfügen. Mit den damit einhergehenden Risiken, die als mögliche Einschränkung von Freiheitsrechten und/oder neuer Kriminalitätsrisiken die Interessen der Bürger als Betroffene unmittelbar und direkt berühren sollten, wird die faktische Nutzung dieser Technologien als Ausdruck von Akzeptanz, zum anderen, zum problematischen Indiz einer neuen Qualität von Überwachung. Vor diesem Hintergrund verfolgte das Projekt, aus dem heraus diese Arbeit entstanden ist, das Ziel am Beispiel des digitalen Fingerabdrucks die Akzeptanz von neuen Kontrolltechnologien zu untersuchen.

Damit verband sich im ersten Teil der Arbeit zuallererst die Frage, wie Akzeptanz gesellschaftlich überhaupt hergestellt wird und mithin, wie der Begriff ausgehend von diesem Unbehagen an der neuen Freiwilligkeit zu verstehen ist. Dabei konnte mit Blick auf seine Konstitution als gesellschaftlichem Schlüsselbegriff und, davon ausgehend, den Zugriff der Akzeptanzforschung ein in mehrfacher Hinsicht normatives Moment der Konsensorientierung identifiziert werden. So ist das Verständnis von Akzeptanz am öffentlich (ausbleibenden) Widerstand orientiert und hat den aufgeklärten, Vor- und Nachteile abwägenden, zumindest subjektiv risikobewussten Bürger vor Augen. Unter der Maßgabe, wie Zustimmungsbereitschaft hergestellt werden kann werden Akzeptanzprobleme, wahrgenommen als Zweck- und Mittelkonflikte, in der Akzeptanzforschung traditionell weggeforscht. Ist der gesellschaftliche Konflikt das Movens der Forschung, hat ihre Zielrichtung, Akzeptanzfähigkeit herzustellen, nämlich ein spezifisches Forschungsprogramm etabliert, in dem die weniger ausdrücklichen Konflikte ebenso ausgeblendet werden, wie auch spezifische, subjektive und politische Beweggründe eine Technologie (nicht) zu nutzen, ungehört bleiben. Die beobachtbare Nutzung einer Technologie wird vielmehr gleichsam zum Ausdruck von Akzeptanz und die Frage, ob (überhaupt) und wie (nicht) akzeptiert und Akzeptanz hergestellt wird, verlagert sich demgegenüber zu einem gesellschaftlichen Gebot dessen, was akzeptiert werden ‚muss'. Die Bedingungen von Akzeptanz werden im Hinblick auf ethische Verantwortbarkeiten in Akzeptanzdiskursen stattdessen auf der Ebene von Akzeptabilitätskriterien verhandelt, die eine Nutzung problematisierter Technologien von vornherein (de-)legitimieren. Vor dem Hintergrund eines

alltagssprachlichen und etymologisch dem *annehmen*, *empfangen* entlehnten Akzeptanzbegriff, wird Akzeptanz dann daraufhin befragt, ob die ihr zugrundeliegenden Gründe „in sich stimmig, schlüssig, sachgemäß, vernünftig, zielführend und insoweit vertretbar, der Situation oder den Verhältnissen angemessen und damit als richtig und rechtens anzuerkennen“ (Lucke 2010: 13)sind. Vor dem Hintergrund der potentiellen Risiken erscheint die Nutzung von Fingerabdrucktechnologien dann kaum vernünftig.

Die Rede über solcherart (vermeintliche) Akzeptanzen steht im Zusammenhang mit den Verständigungsprozessen im Rahmen der Auseinandersetzung mit der Technologie selbst. Im Diskurs um die Fingerabdrucktechnologie entfalten sich nicht nur die konfligierenden Werte, die ihren Einsatz strittig werden lassen, z.B. ihre Bedeutung für Individualität, Privatheit oder Sicherheit und mithin die mit der Technologie einhergehenden Risiken. In der Verhandlung von Akzeptabilitätskriterien wird auch Wissen über die Technologie selbst hervorgebracht. Dabei fungiert das vermeintlich objektive Wirken der Technologie als wechselseitige Argumentationsgrundlage: es bildet in der Regel sowohl die Basis für akzeptanzforcierende als auch Risiken aufzeigende Argumentationen. In den Surveillance Studies führt dies dann dazu, den Einsatz der Fingerabdrucktechnologie nicht nur in Zusammenhängen wie der Aufrechterhaltung von Grenzregimen, sondern als grundsätzlich riskante und unethische ausweisen. Die Frage der Akzeptanz stellt sich für sie folglich ausschließlich negativ, als eine Frage der Kritik, was wiederum eine ihr eigene Normativität begründet. Sie ist damit zudem Bestandteil eines Diskurses, der durch den Bezug auf die funktionalen Versprechen, die sich an die Technologie knüpfen, charakterisiert ist. Aussagen über die (vermeintliche) Akzeptanz, die die Beobachtung der freiwilligenden Datenpreisgabe nahelegen, werden auf der Grundlage der mit der Technologienutzung assoziierten, mithin riskierten, Werte und ihrer vermeintlich objektiven Bedeutung gebildet – dies sowohl auf einer theoretischen, als auch auf der empirischen Ebene.

Vor diesem, im ersten Teil der Arbeit entfalteten Hintergrund, der das Verständnis von Akzeptanz als mithin konstruiertes ausweist, war das Vorgehen der Arbeit darauf ausgerichtet, die Vorannahmen, die Sicherheits- und Risiko- bzw. Überwachungsdiskurse für die Akzeptanz bereitstellen, in einem zweiten Schritt als zumindest Befragbare einzuholen. Mit der Vermutung, dass sich Akzeptanz nicht auf die Einsicht in eine „vernünftige“ Rechtfertigung reduzieren lässt (Lucke 1995: 394), sondern als „Resultat sozialer Konstruktionen“ und Aushandlungsprozesse (ebd. 1998: 20) zu verstehen ist, galt es deshalb, erstens, in Abgrenzung zur traditionellen Akzeptanzforschung und, zweitens, in Anlehnung an phänomenologische,

ethnologische und im weitesten Sinne techniksoziologische Einsichten, nur einige wenige Vorentscheidungen über die Bedingungen und Formen der Akzeptanz selbst zu treffen.

Grundlegender Ausgangspunkt war die Annahme, dass sich beobachtbares Nutzungshandeln nicht zufriedenstellend als eine Frage vorgängiger und mehr oder weniger feststehender Einstellungen erschließt, sondern vielmehr kontextabhängig an soziale Prozesse, z.B. diskursive und interaktive Aushandlungen und kulturelle Alltagspraktiken, gebunden ist. Den Kern der empirischen Untersuchung bildeten 57 leitfadengestützte Interviews mit (potentiellen) Nutzern der Fingerabdrucktechnologie und 185 Beobachtungen von Situationen der Registrierung beziehungsweise der Nutzung des Fingerabdruckverfahrens in unterschiedlichen Anwendungssettings.

Insgesamt konnte die Ausgangsannahme einer Kontextabhängigkeit von Akzeptanz nicht nur bestätigt, sondern auch weiter differenziert werden. Dabei hat sich Akzeptanz vor allem als ein durchaus ambivalentes und vielschichtiges Phänomen erwiesen, das nicht im bloßen Kalkül, das heißt einer mehr oder weniger abrufbaren Abwägung von Vorteilen und Nachteilen, die mit dem Verfahren verbunden werden, aufgeht. Und auch ein sichtbares, scheinbar konformes Handeln ist nicht per se mit Akzeptanz gleichzusetzen. Vielmehr zeugen die Interviews von einer eher komplexen, durchaus Ambivalenzen zulassenden Auseinandersetzung der Nutzer mit der Technologie, die sich im Hinblick auf die Frage persönlicher Relevanzen im Spannungsfeld von Sicherheit vs. Überwachung und rund um das Thema Privatheit bricht.

Im Hinblick auf die Bedeutung der Technologie haben sich zunächst unterschiedliche Ebenen ausmachen lassen, die das Akzeptanzobjekt als ein vielfältiges ausweisen. So variiert eine ihm zugeschriebene Nützlichkeit sowohl mit der technisch-sozialen Einbettung und technologischen Anordnungen im jeweiligen Setting als auch im Vergleich mit anderen Technologien, die ähnliche Zwecke erfüllen. Mit der interpretativen Flexibilität der Technologie im Hinblick auf ihre Anwendung in den jeweiligen Settings ergaben sich nicht nur Einsichten in seine unterschiedlichen Zwecke, sondern auch darin, dass sich die Bedeutung einer Kontrolltechnologie wie des Fingerabdruckverfahrens teilweise erst im Hinblick auf die kulturellen Alltagspraktiken, in die es eingebettet ist – zum Beispiel des Einkaufens im weiteren Sinne oder institutionell-organisatorischen Vorgängen oder auch der Normalität behördlicher Datenerfassung –, verstehen lässt. Ein persönlich relevanter Sinn und Zweck der Technologie erschließt sich folglich vor allem im Vertrauten und die unterschiedlichen Deutungen davon, worauf die Technologie eine Lösung zu bieten vermag, weisen die in klassischen Akzeptanzuntersuchungen vorausgesetzte Zweck-Mittel-Relation als eine kausal vereinfachte Sequenz aus.

Damit variiert dann auch, was überhaupt als Akzeptanzobjekt zu bestimmen ist: Im Supermarkt richtet sich das Handeln auf ein technisches Instrument, welches wiederum in der Automatenvideothek Bestandteil einer größeren Maschinerie ist, über die verfügt wird. Die Integration in größere technische Zusammenhänge zeigte sich auch in den Schulen, in denen explizite Zwecke mitunter lediglich durch das Fingerabdruckverfahren induziert sind. Erst mit seiner Einbindung in ein größeres Abrechnungssystem, in das das bargeldlose Bezahlverfahren Fingerabdruck integriert ist, entfaltet sich sein ‚Angebot', es beispielsweise zum Zweck pädagogisch motivierter Kontrollmotive zu adaptieren. Gerade dort, wo sich der sinnhafte Gebrauch des Verfahrens erst aus dem Zusammenwirken mit anderen technischen Artefakten oder sachtechnischen Systemen ergibt, können sich die Angebotsstrukturen geradezu auch überlagern. Im behördlichen Setting hingegen tritt vor allem der Fingerabdruck selbst als ein Sicherheitsinstrument in den Vordergrund, wenngleich hier seine Bedeutung auch von jener der Ausweisdokumente überlagert sein kann. So unterlaufen die entlang der Argumentationen von Bequemlichkeit und Sicherheit aufscheinenden Facetten der Technologie eine, settingübergreifende, eindeutige Bestimmung des Akzeptanzobjektes – die Eruierung seiner heterogenen Zwecke erwies sich gewissermaßen als eine „Suche nach dem Artefakt" (Tschida 2014).

Die Bedeutung des Objektes wird, dies wurde ebenfalls deutlich, nicht immer entlang eines Wissens erschlossen, das durch Fingerabdrucknehmer bereitgestellt wird. Sinn und Zweck, Vor- und Nachteile der Fingerabdrucktechnologie erschließen sich nicht nur implizit im Setting, sondern auch entlang von Imaginationen, die sich an das Verfahren heften. So zeigt sich auf einer weiteren Ebene der Objektbedeutung, dass sich die Technologie für die Befragten in ein imaginäres Objekt auflöst, an das sich Vorstellungen seines Wirkens knüpfen. In diesem Zusammenhang hat sich gezeigt, dass sich mit der von allen Befragten geteilten Überzeugung von der Objektivität der Technologie – eine eindeutige Identifizierung zu ermöglichen – nicht nur Sicherheitserwartungen verbinden, die mitunter die individuellen Zwecke, die sich jeweils mit der Technologie anschließen, unterlegen. Der Fingerabdruck – fungierend wie ein „Bioskript" – evoziert aber auch Vorstellungen von Unsicherheiten: zum einen dahingehend, wenn etwa mit seiner Nutzung die Gefahr einer fälschlichen Verdächtigung oder das Risiko sich vervielfältigender Profilbildungen verbunden wird oder weil der Fingerabdruck selbst zum Anzeichen einer Unsicherheitslage wird. So schließen sich an das Objekt Szenarien an, die mitunter wie das Wissen vom Fingerabdruck selbst ihren Bezug in literarischen Fiktionen und medialen Diskursen finden, und für die Befragten durchaus real sind. Die zum Ausdruck gebrachten Ambivalenzen lassen sich folglich nicht einfach entlang der Unterscheidung von

objektiv (wahr) oder subjektiv (falsch) bewerten. Vielmehr zeigte sich in diesem Zusammenhang, dass Akzeptanzbereitschaften auf der Verhaltensebene als auch die „guten Gründe“, den Fingerabdruck (nicht) zu nutzen, nicht unbedingt auf gesicherten Annahmen und Informationen über die Technik und deren Verwendung beruhen müssen. Vielmehr plausibilisiert auch das nur vorgestellte, potentiell Mögliche, wie es sowohl der Sicherheitsdiskurs in Form abstrakter Gefährdungslagen als auch der Überwachungsdiskurs im Verweis auf unabsehbare Überwachung im Verweis etwa auf den Orwellschen „Big Brother“ bereitstellen, die Nutzung oder Ablehnung der Technologie. In diesem Zusammenhang ist für das behördliche und schulische Setting die Bedeutung von Angst- und, mitunter gleichwohl durch die symbolische Bedeutung des Verfahrens vermittelten, Sicherheitsdiskursen hervorzuheben, die, vor dem Hintergrund der Ergebnisse, auch zur individuellen Annahme der Technologie beizutragen vermögen, etwa dann, wenn die Technologie als eine Maßnahme der individuellen Sicherheitsvorsorge angesichts unterschiedlicher Unsicherheits- und Ungewissheitsszenarien genutzt wird.

Nicht nur in dieser Hinsicht hat sich erwiesen, dass die Idee des informierten Einverständnisses, des „informed consent“, als Bedingung der Akzeptanz als kaum hinreichend bestimmt werden kann. Seine Begründung findet dieser empirisch belegte Einwand auch nicht allein darin, dass der ‚Durchblick‘ seine Grenze mutmaßlich schon beim technischen Verständnis findet. Bedingungen der Akzeptanz lassen sich überdies nicht in einem vermeintlichen objektiven, d.h. an faktischen Nutzungserfordernissen orientierten, Verhältnis von Freiwilligkeit und Zwang verorten. In dieser Hinsicht variiert Akzeptanz vielmehr, erstens, mit der persönlichen Relevanz der Zwecke der Technologie und in Abhängigkeit von der Legitimität der den Fingerabdrucknehmern jeweils unterstellten Kontrollmotive. In den Schulen führt, zweitens, die ‚fürsorgliche Kontrolle‘, wie sie durch die Einbettung des Fingerabdruckverfahrens in ein Onlinebezahlsystem ermöglicht wird, ein neues Zwangselement ein, das mitunter unabhängig von bürokratischen Bestimmungen ist. Als bestimmend für die Wahrnehmung von Zwang und Freiwilligkeit erweist sich, drittens, die Abhängigkeit von (funktionierender) Technik, welche dann auch Einfluss auf Akzeptanzbereitschaften nimmt, wenn sich etwa im Verlauf der Nutzung die Technologie als widerständig oder die Automatisierung per se als ambivalent erweist. Nicht zuletzt sind die Bedingungen einer konkreten Situation für die Akzeptanz hervorzuheben, die mitunter überhaupt erst Assoziationen hervorrufen und Haltungen buchstäblich erst entstehen lassen. Denn in den Situationen selbst, in denen Nutzer mit dem ihnen häufig zunächst neuen Verfahren konfrontiert werden, vermitteln sich teilweise nicht nur implizit die Zwecke der Fingerabdrucktechnologie, vielmehr kann sich bereits hier auch der Möglich-

keitsraum erschließen, in dem eine Technologie an- beziehungsweise hingenommen oder aber gegebenenfalls auch abgelehnt werden kann. So kann eine Situation etwa als „bekannt“ erlebt werden und sich somit in das Routinewissen (Schütz/Luckmann 2003) über die typischen Abläufe im jeweiligen Setting einfügen. Die, in der traditionellen Akzeptanzforschung zentrale, Frage der Abwägung möglicher Vor- und Nachteile stellt sich dann, zumindest in der konkreten Situation selbst, nicht. Oder, wenn dieses Erfahrungswissen irritiert wird, sind auch etablierte Routinen und insofern auch „situative Zwänge“, wie sie vor allem im behördlichen Setting ausgemacht werden konnten, bestimmend für (Nicht-)Nutzungsentscheidungen. Die Möglichkeit, mit dem Verfahren verbundene Ambivalenzen aufzulösen, kann durch die Anerkennung der Normen der jeweiligen Interaktionsarrangements, etwa in der Position des Antragstellers eines neuen Identitätsdokuments, als unmöglich wahrgenommen werden. Letztere übt dann größeren Einfluss auf die Entscheidung aus, als Zweifel am Sinn und Zweck der Technologie. Diese impliziten Regeln sind dann, ebenso wie das Vertrauen, die eigentlichen Weil-Motive des Handelns (ebd.).

Lässt sich die von den Befragten geäußerte Ambivalenz der Technologie im Sinne eines kritischen Räsonnements auch als Eingabe der politischen Frage in die Diskussion über Kontroll- und Überwachungstechnologien lesen, dann hat die Frage nach der Bedeutung des Fingerabdrucks eine weitere kontextuelle Bedingung der Akzeptanz hervorgebracht. Hier zeigen sich komplexe Einschätzungen zum Thema Privatheit in den Anwendungssettings, bei denen die Interviewten ganz unterschiedliche Vergleichsebenen miteinander verknüpfen, die sowohl den Wert des Datums Fingerabdruck als auch seine Bewertung, mithin Wertigkeit im jeweiligen Setting betreffen. Die Anerkennung eines etwa staatlichen Interesses, beispielsweise die Terrorismusbekämpfung mittels der Erfassung biometrischer Daten, bedeutet nicht gleich, die Frage des Datenschutzes beziehungsweise der Privatheit einem persönlichen Sicherheitsbedürfnis unterzuordnen, wie etwa die Formel einer „willingness to trade off liberties“ (z.B. Bozzoli/Müller 2009) suggeriert. Wie dargestellt orientiert sich die Preisgabe von als persönlich – und darüber hinaus als schützenswert erachteten – Daten vielmehr an kontextuellen Deutungen, denen wiederum, in Anlehnung an Helen Nissenbaums Konzept der „kontextuellen Integrität“ (2004), Vorstellungen einer kontextspezifischen Angemessenheit des Austausches von Informationen zugrunde liegen. Sie sind es, die im Hinblick auf die legitimierten Verwendungsweisen des Fingerabdrucks relevante Orientierungen für eigenes Nutzungshandeln bilden. Erst in dieser Hinsicht lässt sich eruieren, und wie es auch schon die Darstellungen von den heterogenen Zwecken andeuten, die sich für die Nutzer mit der Technologie verbinden, wann die Nutzung des Fingerabdruckverfahrens als (un-)angemessen bewertet wird.

Wenn die Nutzung des Fingerabdruckverfahrens etwa in Bezug auf bestimmte Verhältnisse akzeptabel, für andere jedoch grundsätzlich ausgeschlossen wird, heißt das auch, dass insofern wertorientierte Kongruenzen – in Bezug auf die Qualität des Datums und die vorgestellten Verwendungszwecke – eine Rolle spielen.

Gleichwohl sind es nicht allein die Praxen, die die Bedeutung von Problemfeldern wie Datenschutz oder Überwachung für die Nutzer bestimmen. Diese erweisen sich über die jeweiligen Anwendungssettings hinaus für die Interviewten als durchaus wichtige Themen. Die in der Folge aufscheinende Ambivalenz gegenüber der Technologie wird vor allem durch das spezifische Verhältnis zum Fingerabdrucknehmer moderiert. Folglich kann Akzeptanzkontext dabei so Unterschiedliches wie Anwendungssetting, Situation, soziales Verhältnis oder diskursive Verweisung heißen: Es sind diese Elemente, die sich gleichsam aufeinander beziehen und die die Bedingungen von Akzeptanz hervorbringen: sie sind, wenn man so will, nicht nur zueinander positioniert, sondern sich selbst gleichsam, wenn auch variierend im Hinblick auf ihre jeweils ausschlaggebende Bedeutung, immer auch Kontext, das heißt Umfeld und relationaler Verweis. In Anlehnung an Adele Clarke (2011: 223, Herv. i. O.), die diesen Kontextbegriff für die Analysehaltung der Grounded Theory stark macht, lässt sich also bestimmen, dass sich die „sogenannten kontextuellen Elemente [der Akzeptanz] genau genommen *in der Situation selbst* [befinden]. Sie sind für sie *konstitutiv*, strukturelle und Machtelemente inbegriffen."

Speisen sich die Ambivalenzen der Nutzer vor allem daraus, dass die möglichen Verwendungsweisen der Technologie selbst und die Datennutzungen tendenziell undurchschaut bleiben, hat sich für die Befragten ein Vertrauen, sei es zu Personen oder Institutionen, als wichtig erwiesen, weil es gleichsam das Nicht-Wissen überbrückt. Denn Vertrauen, verstanden als ein „Modus eines Verhältnisses" (Hartmann 2011: 17), bedeutet, bewusst auf vollständiges Wissen zu verzichten (Luhmann 2000), ohne jedoch dabei jeglicher Information zu entsagen. Obwohl sich das Vertrauen implizit durch Erfahrungen aufbaut, explizieren die Nutzer, teilweise offenbar erstmals und für sie selbst überraschend, in den Interviews, mannigfache „gute Gründe" (Baier 2001: 43) für ihr Vertrauen, das wiederum die Nutzung der Technologie rechtfertigt. Vertrauen ermöglicht den Interviewten nicht nur eine Erwartungssicherheit, ohne dass Vor- und Nachteile der Nutzung gegeneinander aufgewogen werden müssen, sondern vielmehr werden Ungewissheiten aufgehoben (Möllering 2006), d.h. die Nutzer befinden sich im Hinblick auf ‚ihr' Anwendungssetting in einer Situation ‚als ob' die mit dem Verfahren verknüpften Ungewissheiten nicht existierten. Das Vertrauen hat sich selbst als akzeptanzmotivierend erwiesen, sei es implizit aufgrund vorgängiger Erfahrungen oder als expliziter Ver-

trauensbeweis, der sich für die Befragten im behördlichen Setting als doppelte Legitimierung staatlichen Kontrollhandelns zeigt. In der ausdrücklichen Übernahme von Verantwortung, dem Staat Vertrauen zu erweisen, konstituieren sich diese Befragten, in Anlehnung Nayars „responsible data-subject“ (2015: 101), als vertrauenswürdige Datensubjekte. Mit dem Vertrauen in der Akzeptanzfrage konkretisieren sich überdies auch die Bedingungen kontextueller Integrität, da es auch darüber Aufschluss gibt, wie weit etwa fürsorgliche Kontrolle reichen darf, und wo, mit Blick auf jenen Ermessenspielraum, nicht nur die Grenzen des Vertrauens, sondern mit ihnen auch jene der Akzeptanz liegen. Insofern spezifizieren insbesondere das Vertrauen unter Vorbehalt und das Misstrauen in staatliche Überwachungspraktiken, die sich in den Interviews nicht nur als Ambivalenz, sondern auch als Differenz zwischen tatsächlicher Fingerabdruckabgabe und kritischen Räsonnement in verschiedenen Facetten gezeigt haben, die Eingabe der politischen Frage in die Diskussion über Kontroll- und Überwachungstechnologien.

Vor diesem Hintergrund hat sich für die Generierung kontextübergreifender Nutzertypen der Vergleich folgender für die Akzeptanz zentraler Merkmale erwiesen: (1) die Handlungsziele, die den Situationen der Antragstellung oder Registrierung zugrunde lagen, (2) die Bedeutung und Anerkennung der vorgestellten Einsatz- und Verwendungszwecke der Technologie sowie (3) die Bedeutung der wahrgenommenen Ambivalenz der Technologie für die eigene Lebenswelt. Weil sowohl den beobachtbaren Nutzungen als auch den Ablehnungen, etwa dann, wenn die Fingerabdrücke nicht in den Personalausweis aufgenommen wurden, nicht immer auch ausdrücklich auf die Technologie bezogene Motivationen zugrunde, bilden (4) wahrgenommene institutionelle und situative Zwänge sowie (5) Vertrauen und Vertrautheit die moderierenden Bedingungen der Akzeptanz.

Ausdrücklich befürwortende Nutzer formulieren ein explizites Eigeninteresse an der Nutzung des Fingerabdrucks und mehrheitlich ein vorgängiges Nutzungsmotiv. Vielfach nehmen sie die angenommenen Zwecke der Technologie als natürliche Kontrollnotwendigkeit für sich an. Dieses übertragene Eigeninteresse kann sowohl idealer als auch eher praktischer Art sein. Es kann darin bestehen, die eigenen Daten vor dem Zugriff Dritter zu schützen oder korrekte Ausweispapiere vorweisen zu können. Zu den ausdrücklich praktischen und im Setting als passend erachteten Zwecken gehört etwa, unabhängig vom Mitführen des Portemonnaies einkaufen zu können oder mit dem bargeldlosen Bezahlverfahren das monatliche Mittagsgeld des Sohnes sicher verwahrt zu sehen. In der Nutzung kann sich aber auch eine Anerkennung politischer Zwecke ausdrücken, wenn die Speicherung der Fingerabdrücke etwa als Beitrag zur Strafverfolgung verstanden wird. Diese Nutzer relativieren vor dem Hintergrund der aner-

kannten Kontrollzwecke einen objektiven Zwang zur Fingerabdruckabgabe bzw. deuten einen solchen in eine Frage der Freiwilligkeit um. Ein ausdrücklich erwiesenes Vertrauen in den Fingerabdrucknehmer erweist sich als sinngebend für diesen Typus. Es neutralisiert vor dem Hintergrund von Glaubwürdigkeit und Nähe nicht nur die durch die Technologie vermittelten Ambivalenzen, sondern ist zuweilen der Grund der Nutzung selbst, zum Beispiel ein freundliches Angebot des Supermarktinhabers anzunehmen oder aber dem Staat explizit Vertrauen zu erweisen. Mehrheitlich findet sich dieser Typus bei den Supermarktkunden und in vergleichsweise geringerem Umfang bei Eltern in den untersuchten Schulen sowie den Antragstellern in der Behörde.

Die ambivalenten Nutzer hingegen können die mit der Technologie verbundene Zwiespältigkeit nur begrenzt auflösen, ohne gleichsam auch die angenommenen, mitunter politischen, Zwecke in Frage zu stellen. Trotz eines Eigeninteresses etwa an Kontrollnotwendigkeiten formulieren sie entweder Vertrauensvorbehalte, so gegenüber der Behörde, wenn etwa der Ausweis mit Fingerabdruck zwar als sicherer gilt, der illegitime Gebrauch der Daten zu Überwachungszwecken durch den Staat aber durchaus angenommen wird. Oder die ambivalenten Nutzer bauen auf die Vertrauenswürdigkeit des Fingerabdrucknehmers etwa in der Videothek, in dessen Verhalten sich zumindest bislang keine Gründe für ein Misstrauen finden ließen bzw. dieser durch Hilfestellungen die mit der Automatisierung einhergehenden Zwänge zumindest abmildert. Ambivalenzen speisen sich für die Nutzer dann auch aus erlebten Abhängigkeiten vom Funktionieren der Technik, wie sie sowohl von Befragten in der Videothek als auch von Schülern problematisiert werden. Vor dem Hintergrund eines solch *ambivalenten Einvernehmens* sind es aber auch situativ erlebte Zwänge, die die Nutzung trotz Unsicherheiten beförderten, wenn etwa (drei) Antragsteller in der Behörde davon absahen, den Sinn und Zweck des Fingerabdrucks zu hinterfragen.

In der Arztpraxis und zu einem großen Teil in der Videothek finden sich die eher *gefälligen Nutzer*. Sie setzen sich weniger zu der Technologie selbst ins Verhältnis, sondern arrangieren sich mit der ohnehin vorhandenen Kontrolle beziehungsweise dem automatisierten Anwendungssetting. Etwaige Ambivalenzen werden im Vertrauen zum Fingerabdrucknehmer aufgehoben und so von vornherein entproblematisiert. Auch in der Behörde findet sich dieser Typus des *gefälligen Hinnehmens*. Diese folgen der Routine und den Vorstellungen eines ‚normalen' Ablaufs in der Behörde und erkennen auch staatliche Kontrollmotive trotz fehlender persönlicher Relevanz an. Insgesamt verbinden sich in diesen Fällen kaum persönliche Zwecke, d.h. Nutzungsmotive, die sich explizit auf die Technologie selbst richten.

Ausdrückliche Ablehner, die sich ausschließlich im behördlichen Setting finden lassen, explizieren ein ausdrückliches Misstrauen. Sie lehnen nicht nur die unterstellten Einsatz- und Verwendungszwecke der Technologie ab, sondern stellen die wollwollenden Motive staatlichen Handelns selbst in Frage.

Aus den Ergebnissen der Untersuchung ergibt sich für die Akzeptanzforschung, dass Akzeptanzhandeln nicht allein aufgrund (expliziter) Handlungsbegründungen erklärt werden kann. Handlungsorientierungen entfalten sich vielmehr vor dem Hintergrund individueller Erfahrungen und situativer Deutungen jeweils in den konkreten Anwendungssettings, aber auch im Verhältnis zu politischen Bedingungen. Bereits in der Frage der Nutzer nach den (unterstellten) Intentionen des Fingerabdrucknehmers verbirgt sich ein „quasipolitisches" Handeln (Hitzler 2001: 45). Akzeptanz folglich als Frage danach zu begreifen, wie und unter welchen Bedingungen sich Bürger kontrovers diskutierte Technologien aneignen, bedeutet auch Widerständigkeit bis hin zur Verweigerung zuzulassen, fallen doch bereits Haltung und Handlung nicht notwendigerweise logisch zusammen (Lucke 1995: 81ff.). So geht die Nutzung der Fingerabdrucktechnologie keineswegs immer auch mit einem vorbehaltlosen Hinnehmen oder gar einem expliziten Annehmen einher – ebenso wie umgekehrt eine kritische Haltung nicht gleich eine faktische Ablehnung der Nutzung nach sich ziehen muss (vgl. in diesem Sinne Lucke 1995: 292). Dabei zeigt sich das Widerständige nicht nur im öffentlichen Infragestellen, gar Attackieren, von Technologien, sondern auch im kleinlauten Protest oder manchmal auch im stummen Unbehagen, der bzw. das sich, wie in den Interviews geäußert, mitunter hinter dem scheinbar widerspruchslosen Akzeptieren verbergen kann.

Akzeptanzforschung sollte daher Ambivalenz und Ambiguität für die Analyse fruchtbar machen, statt den Konflikt, der ihre Ursache und ihr Motiv bildet, gleichsam wegzuforschen. Das bedeutet dann, das Subjekt der Aneignung von Technologien in den Mittelpunkt zu stellen und zu fragen, wie es sich als solches innerhalb von sozio-technischen Ordnungen und Anordnungen artikuliert und diese seinerseits mitkonstituiert. Zu befragen gälte in diesem Zusammenhang dann auch der vermeintlich objektive Sinn von Technologien, mithin die ‚Realität' der ‚anzunehmenden' Objekte, die mitunter zwischen „symbolisch-kommunikativer" und „praktisch-materieller Wirksamkeit" (Braun-Thürmann 2006: 217) oszilliert. Auf diese Weise ließe sich auch erhellen, was sich hinter dem vermeintlichen „Mangel an Konsistenz" (Renn 2005: 31) verbirgt, den eine vorrangig an Akzeptabilitätskriterien orientierte Akzeptanzforschung mit Blick auf die scheinbar widersprüchlichen Haltungen der Bürger gegenüber unterschiedlichen „Technikbereichen" moniert, mithin beklagen muss.

Den Ausgangspunkt gerade an jenen scheinbar irrationalen Akzeptanzlagen zu nehmen, würde dann auch bedeuten, in einer Weise am Dissens von ‚Experten' und ‚Laien' anzusetzen, die weniger auf Konsistenzüberlegungen zielt, unterschiedliche Risiken miteinander in Beziehung zu setzen, sondern auch den Rationalitätsanspruch erster in Augenschein zu nehmen. Gerade der Blick auf den Sicherheitsdiskurs, der in der Akzeptanzforschung bislang wenig Berücksichtigung gefunden hat, und als Angstdiskurs die Einführung und Durchsetzung von Kontroll- und Überwachungstechnologien fundieren kann (vgl. Traut et al. 2010), kann die Aufmerksamkeit dafür schärfen, wie reale Ereignisse, gesellschaftliche Imaginationen von Bedrohungen und das Versprechen von Sicherheitstechnologien miteinander verknüpft werden. Es wären aber nicht nur Sicherheitsdiskurse als Voraussetzungen von Akzeptanz mit in die Untersuchung einzubeziehen, um auf diese Weise grundlegender auch das (sich verändernde) Verhältnis von Gesellschaft, Überwachungstechnologien und Staat in den Blick zu nehmen, sondern auch jene kritischen Diskurse, die ebenfalls die Akzeptanzfrage mitkonturieren. Denn wirft das Vorhandensein von Überwachung ermöglichenden Technologien regelmäßig die Frage nach dem Verhältnis zwischen Sicherheit und Freiheit auf, ist ein damit verbundener Ausgleichsgedanke aber nicht nur problematisch „wenn deutlich wird, dass diese Preise überhöht sind, oder wenn der Verdacht besteht, dass der Gegenwert nicht in der erhofften Form vorhanden ist" (Ammicht-Quinn 2014: 29). So sind Sicherheit und Risiko selbst nicht objektiv gegeben, sondern wandelbare gesellschaftliche Reflexionsgrößen und zu bestimmen ist zudem, welche „Bedeutung" etwa dem Vorhandensein von Schutz, die Abwesenheit von Gefahr oder die Gewissheit der Zuverlässigkeit von Schutz „vor dem Horizont historischer, individueller und sozialer Kontexte zukommt" (ebd.: 24). Insofern müsste Akzeptanzforschung auch darauf zielen, den „rhetorical smoke screen" (Monahan 2006: 2) nicht nur im affirmativen, sondern auch im kritischen Diskurs aufzulösen, der die Akzeptanz von ‚Sicherheits'- und ‚Überwachungs'technologien im Verhältnis von Sicherheit und Freiheit zementiert und der, in seinem Bezug auf imaginäre Vorstellungswelten, das Wissen von Technologien bereitstellt und dabei, zumindest im Beispielfeld der Fingerabdrucktechnologie, riskiert, jenes vom vermeintlich objektiven Wirken von Technologien zu reproduzieren.

Fungiert der kritische Diskurs insofern als ein weiterer Akteur von Akzeptanzpolitik, der – indem er, die ideologische Debatte über die Dissense zwischen Experten und Laien bei der Beurteilung von Risiken fortführend, darauf zielt, individuelle Einstellungen durch ein Mehr an und ‚bessere' Informationen zu beeinflussen –, letztlich auch die Kriterien bereitstellt, an denen Akzeptanz bemessen wird, dann sollte Akzeptanzforschung, nicht zuletzt, auch den Begriff der Akzeptanz selbst befragen. So bildet die Vorstellung von Akzeptanz selbst ein

spezifisches Moment in einem je gesellschaftlich-historischen Kontext (vgl. Lucke 1995: 98). Man kann, auch wenn Lucke dies nicht in einer in diesem Sinne gänzlich konstruktivistischen Perspektive andeutet, argumentieren, dass das Konzept der Akzeptanz selbst das „Resultat umfassender Prozesse der kollektiven und individuellen Aneignung kulturell-gesellschaftlicher Entäußerungen“ (ebd.: 102) darstellt. So verbindet sich die Karriere des Akzeptanzbegriffes mit der Erkenntnis, dass Rationalisierungskonflikte nicht mehr nur auf der Ebene der institutionellen oder strukturellen Legitimation verortet werden können, sondern sich eben auch auf der „subjektiv-sozialen“ Ebene stellen (ebd.: 19). Die Bedeutung von Akzeptanzfragen und Akzeptanzbefragungen liegt, bei aller Uneindeutigkeit des Begriffs selbst, darin, dass ihre Ergebnisse nicht nur als Indikatoren einer „gesellschaftlichen Grundstimmung“ (ebd.: 15) oder eines „Meinungsklima“ (Jaufmann 1999: 208) gelten. Mit ihnen sollen zudem sichere Zustimmungswerte einer unsicheren Zukunft und gleichsam zu begründenden Gegenwart ermittelt werden (vgl. Lucke 1995: 14f.). Will man Akzeptanz also weiterhin als Leitthema der „gesellschaftlichen Selbstthematisierung“ (ebd.: 16) ernstnehmen, dann muss dies auch mit einer kritischen Reflexion der der Akzeptanzforschung eigenen Rationalität einhergehen. Denn mit der Vereinnahmung in ihren Verwendungszusammenhang, mitunter auch in eine als ‚Heilungsbedürfnis‘ zu charakterisierende Rationalität, gerät nicht nur aus dem Blick, ob etwa Akzeptanz zugleich aktive Annahme oder ‚bloß‘ Hinnahme oder Tolerierung bedeutet, sondern auch welche spezifischen, subjektiven und politischen Beweggründe den gesellschaftlichen Konflikten vielleicht zugrunde liegen. Solange sich Akzeptanzforschung nicht einem solchen „Kontrastprogramm“ (ebd.: 338) zuwendet, sieht sie sich jedoch entsubjektiviert und entpolitisiert.

Literaturverzeichnis

Aas, Katja Franko (2011): 'Crimmigrant' bodies and bona fide travelers: Surveillance, citizenship and global governance. In: Theoretical Criminology 3(15): 331-346

Aas, Katja Franko (2006): The body does not lie: Identity, risk and trust in technoculture. In: Crime, Media, Culture: An International Journal 2(2): 143-158

Aas, Katja Franko (2004): From narrative to database: Technological change and penal culture. In: Punishment & Society 6(4): 379-393

Acquisti, Alessandro/Jens Grossklags (2004): Privacy Attitudes and Privacy Behaviour. Losses, Gains and Hyperbolic Discounting. In: L. Jean Camp/Stephen Lewis (Hg.): The Economics of Information Security. Boston et al.: Kluwer Academic Publication: 165-178

Adloff, Frank/Steffen Mau (2005): Zur Theorie der Gabe und Reziprozität. In: Diess. (Hg.): Vom Geben und Nehmen. Zur Soziologie der Reziprozität. Frankfurt a.M./New York: Campus Verlag: 9-57

Ajzen, Icek (1985): From intentions to actions: A theory of planned behavior. In Julius Kuhl/Jürgen Beckmann (Hg.): Action Control: From cognition to behavior. Heidelberg: Springer: 11-39

Akrich, Madeleine (1995): User Representations: Practices, Methods and Sociology. In: Arie Rip/Thomas J. Misa/Johan W. Schot (Hg.): Managing Technology in Society. London/New York: Pinker Publishers: 167-184

Akrich, Madeleine (1992): The De-Scription of Technical Objects. In: Wiebe Bijker/John Law (Hg.): Shaping Technology/Building Society. London: The MIT Press: 205-224

Albrecht, Astrid (2002): Relevanz biometrischer Verfahren im gesellschaftlichen Kontext. In: Veronika Nolde/Lothar Leger (Hg.): Biometrische Verfahren. Körpermerkmale als Passwort - Grundlagen, Sicherheit und Einsatzgebiete. Köln: Dt. Wirtschaftsdienst: 85-96

Albrecht, Hans-Jörg (2008): Kosten und Nutzen technischer Überwachung: In: Sandro Gaycken/Constanze Kurz (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: transcript Verlag: 129-147

Al-Harby, Fahad/Rami Qahwaji/Mumtaz Kamala (2010): Towards an Understanding of User Acceptance to Use Biometrics Authentication Systems in E-Commerce: Using an Extension of the Technology Acceptance Model. In: International Journal of E-Business Research 6(3): 34-55

Alterman, Anton (2003): "A piece of yourself": Ethical issues in biometric identification. In: Ethics and Information Technology 5(3): 139-150

Amoore, Louise (2008): Governing by identity. In: Colin J. Bennett/David Lyon (Hg.): Playing the identity card. Surveillance, security and identification in global Perspective. Routledge: London: 21-36

Ammicht-Quinn, Regina (2014): Sicherheitsethik. Eine Einführung. In: Dies. (Hg.): Sicherheitsethik. Wiesbaden: Springer VS: 15-50

Ammicht-Quinn, Regina/Benjamin Rampp (2009): "It'll turn your heart black you can trust": Angst, Sicherheit und Ethik. In: Vierteljahrshefte zur Wirtschaftsforschung 78(4): 136–149

Anderson, Ben (2009) Affective atmospheres. In: Emotion, Space and Society 2(2): 77-81

Arendt, Hannah (1999): Vita activa oder Vom tätigen Leben. München: Pieper Taschenbuch Verlag

Aus, Jonathan P. (2008): EU Governance in an Area of Freedom, Security and Justice. Logics of Decision-making in the Justice and Home Affairs Council. Ph.D.Dissertation. Oslo: University of Oslo. Online verfügbar unter: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.6588&rep=rep1&type=pdf [14.07.2015]

Aus, Jonathan P. (2006): Decision-making under Pressure: The Negotiation of the Biometric Passports Regulation in the Council. Arena Working Paper No. 11. Online verfügbar unter: http://www.sv.uio.no/arena/english/research/publications/arena-working-papers/2001-2010/2006/wp06_11.pdf [13.04.2012]

Baccelli, Emmanuel et al. (2012): SAFEST: A Framework for Early Security Triggers in Public Spaces. Workshop Interdisciplinaire Sur la Sécurité Globale (WISG), Jan 2012, Troyes, France. Online verfügbar unter: https://hal.inria.fr/hal-00666698 [15.06.2014]

Baier, Annette (2001): Vertrauen und seine Grenzen. In: Martin Hartmann/Claus Offe (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt a.M./New York: Campus: 37-84

Ball, Kirstie (2009): Exposure. Exploring the subject of surveillance. In: Information, Communication & Society 12(5): 639-657

Barben, Daniel (2010a): Acceptance Politics. In: David H. Guston (Hg.): Encyclopedia of Nanoscience and Society. Vol. 1. Thousand Oaks/Cal.: Sage Reference: 4-5

Barben, Daniel (2010b): Analyzing acceptance politics: Towards an epistemological shift in the public understanding of science and technology. In: Public Understanding of Science 19(3): 274-292

Barber, Bernard (1983): The Logic and Limits of Trust. New Brunswick/New York: Rutgers University Press

Barnard-Wills, David (2011): UK News Media Discourses of Surveillance. In: The Sociological Quarterly 52(4): 548-567

Barnard-Wills, David/Helen Wells (2012): Surveillance, technology and the everyday. In: Criminology and Criminal Justice 12(3): 227-237

Barthes, Roland (1990): Der entgegenkommende und der stumpfe Sinn. Frankfurt a.M.: Suhrkamp

Bäumler, Helmut/Lukas Gundermann/Thomas Probst (2001): Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen. Online verfügbar unter: https://www.datenschutzzentrum.de/download/tabga.pdf [10.09.2014]

Bechmann, Gotthard (1997): Einleitung: Risiko – ein neues Forschungsfeld? In: Ders. (Hg.): Risiko und Gesellschaft. Grundlagen und Ergebnisse interdisziplinärer Risikoforschung. Opladen: Westdeutscher Verlag: VII-XXIX

Beck, Stefan (1997): Umgang mit Technik. Kulturelle Praxen und kulturwissenschaftliche Forschungskonzepte. Berlin: Akademie Verlag

Becker, Peter (2005): Dem Täter auf der Spur: Eine Geschichte der Kriminalistik. Darmstadt: Wissenschaftliche Buchgesellschaft

Beier, Rosmarie (1990): Der gläserne Mensch - eine Sensation: zur Kulturgeschichte eines Ausstellungsobjekts. Stuttgart: Hatje

Berg, Charles/Marianne Milmeister (2008): Im Dialog mit den Daten das eigene Erzählen der Geschichte finden. Über die Kodierverfahren der Grounded-Theory-Methodologie [47 Ab-

sätze]. Forum Qualitative Sozialforschung 9(2), Art. 13. Online verfügbar unter: https://www.ssoar.info/ssoar/handle/document/9106 [13.05.2017]

Berger, Peter L./Thomas Luckmann (1980): Die gesellschaftliche Konstruktion der Wirklichkeit. Eine Theorie der Wissenssoziologie. Frankfurt a.M.: S. Fischer Verlag GmbH

Berlinghoff, Marcel (2013): Computerisierung und Privatheit – Historische Perspektiven. In: Aus Politik und Zeitgeschichte 63(15/16): 14-19

Bernfeld, Siegfried (1996): Die Tantalus-Situation. Bemerkungen zum „kriminellen Über-Ich“. In: Ders.: Sämtliche Werke. Bd. 11. Weinheim/Basel: Beltz: 303-321

Bigo, Didier (2002): Security and immigration: Toward a critique of the governmentality of unease. In: Alternatives: Global, Local, Political 27: 63-92

Bijker, Wiebe/John Law (1992): General Introduction. In: Diess. (Hg.): Shaping Technology/Building Society. London: The MIT Press: 1-16

Blumer, Herbert (2004): Der methodologische Standort des symbolischen Interaktionismus. In: Jörg Strübing/Bernd Schnettler (Hg.): Methodologie interpretativer Sozialforschung. Klassische Grundlagentexte. Konstanz: Universitätsverlag Konstanz: 319-385

Bogner, Alexander/Wolfgang Menz (2005): Das theoriegenerierende Experteninterview. Erkenntnisinteresse, Wissensformen, Interaktion. In: Alexander Bogner/Beate Littig/Wolfgang Menz (Hg.): Das Experteninterview. Theorie, Methode, Anwendung. Wiesbaden: Springer VS: 33-70

Bonß, Wolfgang (1996): Die Rückkehr der Unsicherheit. Zur gesellschaftstheoretischen Bedeutung des Risikobegriffs. In: Georg Banse (Hg.): Risikoforschung zwischen Disziplinarität und Interdisziplinarität. Von der Illusion der Sicherheit zum Umgang mit Unsicherheit. Opladen: Westdeutscher Verlag: 165-192

Bonß, Wolfgang (1995): Vom Risiko. Unsicherheit und Ungewißheit in der Moderne. Hamburg: Hamburger Edition

Bonß, Wolfgang/Katrin Wagner (2012): Risiken und symbolische Politik: Anmerkungen zu einem Konzept und seiner Bedeutung für die Luftsicherheit. In: Lars Gerhold/Jochen Schiller (Hg.): Perspektiven der Sicherheitsforschung: Beiträge aus dem Forschungsforum Öffentliche Sicherheit. Frankfurt et al.: Peter Lang: 41-53

Bourdieu, Pierre (1983): Ökonomisches Kapital, kulturelles Kapital, soziales Kapital. In: Reinhard Kreckel (Hg): Soziale Ungleichheiten. Soziale Welt. Sonderband 2. Göttingen: Schwartz: 183-198

Bozzoli, Carlos/Cathérine Müller (2009): Perceptions and Attitudes to a Terrorist Shock. Evidence from the UK. Economics of Security Working Paper 13. Berlin: Economics of Security. Online verfügbar unter: http://www.diw.de/documents/publikationen/73/diw_01.c.354140.de/diw_econsec0013.pdf [15.02.3014]

Breitenstein, Marco (2002): Überblick über biometrische Verfahren. In: Veronika Nolde/Lothar Leger (Hg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete. Köln: Deutscher Wirtschaftsdienst: 35-82

Bröckling, Ulrich (2012): Dispositive der Vorbeugung: Gefahrenabwehr, Resilienz, Precaution. In: Christopher Daase/Philipp Offermann/Valentin Rauer (Hg.): Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr. Frankfurt a.M.: Campus: 93-108

Bröckling, Ulrich (2004): Prävention. In: Ders./Susanne Krasmann/Thomas Lemke (Hg.): Glossar der Gegenwart. Frankfurt a.M.: Suhrkamp: 210-215

Bromba, Manfred (2007): Ein biometrisches Bezahlsystem für Kaufhäuser. In: Datenschutz und Datensicherheit 31(3): 194-198

Bug, Michael/Katrin Wagner (2015): Der digitalisierte Passagier. In Stephan Humer (Hg.): Terrorismus A/D: Wechselwirkungen zwischen analoger und digitaler Sphäre. Reihe Digitale Wissenschaft. Winnenden: CWS Verlag

Bug, Michael/Ursula Münch (2012): Politik verändert Internet (und Medien) – Innere Sicherheit, Vorratsdatenspeicherung und die Wahrnehmung durch die Bevölkerung. In: Michael Schröder (Hg.): Die Web-Revolution. Das Internet verändert Politik und Medien. München: Olzog: 147-174

Büllingen, Franz/Annette Hillebrand (2000): Biometrie als Teil der Sicherungsinfrastruktur? In: Datenschutz und Datensicherheit 24(2): 339-343

Butt, Arslan (2011): "I might not scratch my ass if I think there might be a camera taping it": Public Perception of Surveillance Technologies in Everyday Life. In: Cyber-Surveillance in Everyday Life: An International Workshop 12.-15.05.2011. University of Toronto. Online verfügbar unter: http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Butt-I-might-not-scratch.pdf [16.07.2013]

Buzan, Barry/Ole Wæver/Jaap de Wilde (1998): Security: A New Framework for Analysis. Boulder: Lynne Reinner

Caplan, Jane (2001): "This or That Particular Person": Protocols of Identification in Nineteenth-Century Europe. In: Dies./John Torpey (Hg.): Documenting Individual Identity. Princeton/Oxford: Princeton University Press: 49-66

Capurro, Rafael (2008): Zwischen Vertrauen und Angst. Über Stimmungen der Informationsgesellschaft. In: Dieter Klumpp/Herbert Kubicek/Alexander Roßnagel/Wolfgang Schulz (Hg.): Informationelles Vertrauen für die Informationsgesellschaft. Berlin/Heidelberg: Springer-Verlag: 53-62

Ceyhan, Ayse (2008): Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. In: Surveillance & Society 5(2): 102-123. Online verfügbar unter: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3430/3393 [15.06.2014]

Clarke, Adele (2011): Von der Grounded-Theory-Methodology zur Situationsanalyse. In: Günter Mey/Katja Mruck (Hg.): Grounded Theory Reader. Wiesbaden: VS Verlag für Sozialwissenschaften: 207-229

Clarke, Roger (1988): Information Technology and Dataveillance. Online verfügbar unter: http://www.rogerclarke.com/DV/CACM88.html [25.06.2016]

Clodfelter, Richard (2010): Biometric technology in retailing: Will consumers accept fingerprint authentication? In: Journal of Retailing and Consumer Services 17(3): 181-188

Cole, Simon (2008): The 'Opinionization' of Fingerprint Evidence. In: BioSocieties 3(1): 105-113

Cole, Simon (2005): More than Zero: Accounting for Error in Latent Fingerprint Identification. In: The Journal of Criminal Law and Criminology 95(3): 985-1078

Cole, Simon (2002): Suspect identities. A history of fingerprinting and criminal identification. Cambridge: Harvard University Press

Cole, Simon/Rachel Dioso-Villa (2009): Investigating the ‚CSI Effect' Effect: Media and Litigation Crisis in Criminal Law. In: Stanford Law Review 61(6): 1335-1374

Cole, Simon/Henry N. Pontell (2006): “Don’t Be Low Hanging Fruit”. Identity Theft as Moral Panic. In: Torin Monahan (Hg.): Surveillance and Security: technological politics and power in everyday life. New York/Oxon: Routledge: 125-147

Coleman, James (1991): Grundlagen der Sozialtheorie. Band 1: Handlungen und Handlungssysteme. München: Oldenbourg

Conze, Eckart (2012): Securitization. Gegenwartsdiagnose oder historischer Analyseansatz? In: Geschichte und Gesellschaft 38(3): 453-467

Daston, Lorraine/Peter Galison (2009): Objectivity. New York: Zone Books

Davis, Fred D. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. In: MIS Quarterly 13(3): 319-339

Degenhardt, Werner (1986): Akzeptanzforschung zu Bildschirmtext – Methoden und Ergebnisse. München: Reinhard Fischer

Dellwing, Michael/Robert Prus (2012): Einführung in die interaktionistische Ethnografie. Soziologie im Außendienst. Wiesbaden: Springer VS

Deppermann, Arnulf (2008): Gespräche analysieren. Eine Einführung. Wiesbaden: VS Verlag für Sozialwissenschaften

Deppermann, Arnulf/Thomas Spranz-Fogasy („001): Aspekte und Merkmale der Gesprächssituation. In: Klaus Brinker/Gerd Antos/Wolfgang Heinemann/Sven F. Sager (Hg.): Text- und Gesprächslinguistik. Ein internationales Handbuch zeitgenössischer Forschung. Berlin/New York: de Gruyter: 1148-1161

Dethloff, Claus (2004): Akzeptanz und Nicht-Akzeptanz von technischen Produktinnovationen. Lengerich et al.: Pabst Science Publishers

Diekmann, Andreas (2000): Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen. Reinbek bei Hamburg: Rowohlt

Dierkes, Meinolf/Lutz Marz (1993): Anstelle einer Einführung: Technikakzeptanz, Technikfolgen und Technikgenese. Zur Weiterentwicklung konzeptioneller Grundlagen der sozialwissenschaftlichen Technikforschung. In: Meinolf Dierkes (Hg.): Die Technisierung und ihre Folgen. Zur Biographie eines Forschungsfeldes. Berlin: Ed. Sigma: 17-44

Easton, David (1975): A Re-Assessment of the Concept of Political Support. In: British Journal of Political Science 5(4): 453-457

Ehmke, Wolfgang (1987): 10 Jahre Gorleben – (k)ein Grund zum Feiern? In: Ders. (Hg.): Zwischenschritte. Die Anti-Atomkraft-Bewegung zwischen Gorleben und Wackersdorf. Köln: Köln Volksblatt Verlag: 9-12

Ehrenberg-Silies, Simone/Martin Hering/Hannes Kurtze/Marc Bovenschulte (2012): Technikfolgenabschätzung neu denken. In: iit perspektive. Working Paper des Instituts für Innovation und Technik 10: 1-9. Online verfügbar unter: https://www.iit-berlin.de/de/publikationen/iit-perspektive-10/at_download/download [16.07.2016]

Eisch-Angus, Katharina (2009): Sicher forschen? Methodische Überlegungen zum Ethnografieren von Sicherheit und Alltag. In: Sonja Windmüller/Beate Binder/Thomas Hengartner (Hg.): Kultur - Forschung. Zum Profil einer volkskundlichen Kulturwissenschaft. Münster et al.: Lit Verlag: 69-90

Eisenberg, Ulrich/Jens Puschke/Tobias Singelnstein (2005): Ubiquitäres Computing = ubiquitäre Kontrolle? In: Kriminologisches Journal 37(2): 93-108

Eisenegger, Mark (2005): Reputation in der Mediengesellschaft. Konstitution – Issues – Monitoring – Issues Management. Wiesbaden: VS Verlag für Sozialwissenschaften

Eisenstadt, Shmuel N. (2001): Vertrauen, kollektive Identität und Vertrauen. In: Martin Hartmann/Claus Martin (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt a.M.: Campus: 333-363

Ellerbrok, Ariane (2011): Playful Biometrics. Controversial Technology through the Lens of Play. In: The Sociological Quarterly 52(4): 528-547

Ellis, Darren (2011): Islamophobia and Ontological Insecurity: The Impacts of Impersonal Trust upon Interpersonal Trust. In: Research and Practice in Social Science 7(1): 1-16

Elm, Theo (1991): Funktionen der Literatur in der technischen Kultur. In: Ders./Hans H. Hiebel (Hg.): Medien und Maschinen. Literatur im technischen Zeitalter. Freiburg: Rombach Verlag: 47-69

Endreß, Martin (2012): Vertrauen und Misstrauen – Soziologische Überlegungen. In: Christian Schilcher/Macha Will-Zocholl/Marc Ziegler (Hg.): Vertrauen und Kooperation in der Arbeitswelt. Wiesbaden: VS Verlag für Sozialwissenschaften: 81-102

Endreß, Martin (2008): Fungierendes Vertrauen – Eine prä-reflexive wie meta-reflexive Ressource. Vortrag. Berlin Juli 2008.
Online verfügbar unter: http://www.bildungsvertrauen.de/material/endress_nw1.pdf [15.04.2014]

Endreß, Martin (2002): Vertrauen. Bielefeld: transcript-Verlag

Endreß, Martin (2001): Vertrauen und Vertrautheit – Phänomenologisch-anthropologische Grundlegung. In: Martin Hartmann/Claus Martin (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt a.M.: Campus: 161-203

Endreß, Martin/Benjamin Rampp (2013): Vertrauen in der Sicherheitsgesellschaft. In Sitzungsberichte der Leibnitz-Sozietät der Wissenschaften zu Berlin 116: 145-160. Online verfügbar unter: http://leibnizsozietaet.de/wp-content/uploads/2013/06/13_endress-rampp.pdf [22.08.2013]

Endruweit, Günter (2014): Akzeptanz und Sozialverträglichkeit. In: Ders./Gisela Trommsdorf (Hg.): Wörterbuch der Soziologie. Stuttgart: Lucius & Lucius: 6-7

Englert, Carina Jasmin (2014): Der CSI-Effekt in Deutschland. Die Macht des Crime-TV. Wiesbaden: Springer VS

Ericson, Richard V./Kevin D. Haggerty (1997): Policing the risk society. Oxford: Clarendon

Esposito, Elena (2007): Die Fiktion der wahrscheinlichen Realität. Frankfurt a.M.: Suhrkamp

Ewald, Francois (1998): Die Rückkehr des genius malignus: Entwurf zu einer Philosophie der Vorbeugung. In: Soziale Welt 49(1): 5-23

Feest, Johannes/Blankenburg, Thomas 1972: Die Definitionsmacht der Polizei. Düsseldorf: Bertelsmann

Felt, Ulrike/Maximilian Fochler (2009): Between the Fat-pill and the Atomic Bomb: Civic Imaginations of Regimes of Innovation Governance. In: Science as Culture 20(3): 307-328

Felt, Ulrike/Brian Wynne (2007): Taking European knowledge society seriously. Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission. Luxembourg: Office for Official Publications of the European Communities. Online verfügbar unter:

https://ec.europa.eu/research/science-society/document_library/pdf_06/european-knowledge-society_en.pdf [13.06.2015]

Feltes, Thomas/Dominic Kudlacek/Andreas Ruch (2013): Schlussbericht zum Verbundprojekt: Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme (APFel). Teilvorhaben der Ruhr-Universität Bochum. Untersuchungen zum Sicherheitsgefühl sowie zur Akzeptanz, Nutzerfreundlichkeit und Datenschutz. Bochum: Ruhr Universität Bochum

Fishbein, Martin/Icek Ajzen (1975): Belief, attitude, intention, and behavior: An introduction to theory and research. Reading/MA: Addison-Wesley

Flick, Uwe (2011): Triangulation: eine Einführung. Wiesbaden

Flick, Uwe (2007): Qualitative Forschung. Eine Einführung. Reinbek bei Hamburg: Rowohlt

Flick, Uwe (2005): Triangulation. In: Ders./Ernst von Kardorff/Ines Steinke (Hg.): Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg: Rowohlt: 309-318

Flick, Uwe (1996): Psychologie des technisierten Alltags. Opladen: Westdeutscher Verlag

Fotel, Trine/Thyra Uth Thomsen (2004): The Surveillance of Children's Mobility. In: Surveillance and Society 1(4): 535-554

Foucault, Michel (1998): Überwachen und Strafen. Frankfurt a.M.: Suhrkamp

Foucault, Michel (1992): Was ist Kritik? Berlin: Merve

Frevert, Ute (2013): Vertrauensfragen. Eine Obsession der Moderne. München: C.H. Beck

Frey, Bruno S./Matthias Benz/Alois Stutzer (2004): Introducing Procedural Utility: Not Only What, but Also How Matters. In: Journal of Institutional and Theoretical Economics 160: 377-401

Friesen, Norm/Andrew Feenberg/Grace Smith (2009): Phenomenology and Surveillance Studies. Returning to the things themselves. In: The Information Society: An International Journal 25(2): 84-90

Froschauer, Ulrike/Manfred Lueger (2003): Das qualitative Interview. Zur Praxis interpretativer Analyse sozialer Systeme. Wien: UTB

Fuchs, Christian (2015): Surveillance and Critical Theory. In: Media and Communication 3(2): 6-9

Fuchs, Dieter (2002): Die politische Theorie der Systemanalyse: David Easton. In: Andre Brodocz/Gary S. Schaal (Hg.): Politische Theorien der Gegenwart I. Opladen: Leske + Budrich: 345-370

Fuchs-Heinritz, Werner (1995a): Legitimität. In: Ders./Rüdiger Lautmann/Otthein Rammstedt/Hanns Wienold (Hg.): Lexikon der Soziologie. Opladen: Westdeutscher Verlag: 396

Fuchs-Heinritz, Werner (1995b): Protest, politischer. In: Ders./Rüdiger Lautmann/Otthein Rammstedt/Hanns Wienold (Hg.): Lexikon der Soziologie. Opladen: Westdeutscher Verlag: 525

Fuhse, Jan A. (2002): Kann ich dir vertrauen? Strukturbildung in dyadischen Sozialbeziehungen. In: Österreichische Zeitschrift für Politikwissenschaft 31(4): 413-426

Furedi, Frank (2005): The Politics of Fear. London et al.: Continuum

Gabriel, Oscar W. (1993): Institutionenvertrauen im vereinigten Deutschland. Aus Politik und Zeitgeschichte 54: 3-12

Gambetta, Diego (2001): Können wir dem Vertrauen vertrauen? In: Martin Hartmann/Claus Offe (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt a.M./New York: Campus: 204-237

Garfinkel, Harold (1967): Studies in Ethnomethodology. Englewood Cliffs: Prentice-Hall

Garland, David (2001): The Culture of Control, Crime and Social Order in Contemporary Society. Chicago/Oxford: University of Chicago Press

Garland, David (1997): ‚Gouvernmentality' and the Problem of Crime: Foucault, Criminology, Sociology. In: Theoretical Criminology 1(2): 173-214

Gates, Kelly (2013): The cultural labour of surveillance: video forensics, computational objectivity, and the production of visual evidence. In: Social Semiotics 23(2): 242-260

Gates, Kelly (2006): Identifying the 9/11 'Faces of terror'. The promise and problem of facial recognition technology. In: Cultural Studies 20(4-5): 417-440

Gates, Kelly (2005): Biometrics and Post-9/11 Technostalgia. In: Social Text 83(2): 35-53

Gerhold, Lars/Marie-Luise Beck/Jochen Schiller (2012): Zwischen Sicherheit und Unsicherheit. Herausforderungen eines interdisziplinären Diskursfeldes. In: Lars Gerhold/Jochen Schiller (Hg.): Perspektiven der Sicherheitsforschung: Beiträge aus dem Forschungsforum Öffentliche Sicherheit. Frankfurt et al.: Peter Lang: 13-26

Giddens, Anthony (1995): Konsequenzen der Moderne. Frankfurt a.M.: Suhrkamp

Ginzburg, Carlo (1995): Spurensicherung: Die Wissenschaft auf der Suche nach sich selbst. Berlin: Wagenbach

Glaeßner, Gert-Joachim (2010): Die Innen- und Rechtspolitik der Großen Koalition. In: Sebastian Bukow/Wenke Seemann (Hg.): Die Große Koalition. Regierung – Politik – Parteien 2005–2009. Wiesbaden: VS Verlag für Sozialwissenschaften: 174-190.

Glaser, Barney G./Anselm L. Strauss (1998): Grounded Theory: Strategien qualitativer Forschung. Bern: Huber

Gläser, Joachim/Grit Laudel (2010): Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen. Wiesbaden: VS Verlag für Sozialwissenschaften

Gloede, Fritz/Leonhard Hennen (2005): Technikakzeptanz als Gegenstand wissenschaftlicher und politischer Diskussionen. Eine Einführung in den Schwerpunkt. In: Technikfolgenabschätzung. Theorie und Praxis. 14(3): 4-12

Goffman, Erving (2010): Stigma: Über Techniken der Bewältigung beschädigter Identität. Frankfurt a.M.: Suhrkamp

Goffman, Erving (2009): Interaktion im öffentlichen Raum. Frankfurt a.M.: Campus Verlag.

Goffman, Erving (1977): Rahmen-Analyse: Ein Versuch über die Organisation von Alltagserfahrungen. Frankfurt a.M.: Suhrkamp

Goffman, Erving (1974): Das Individuum im öffentlichen Austausch. Mikrostudien zur öffentlichen Ordnung. Frankfurt a.M.: Suhrkamp

Goold, Benjamin (2010): Consuming security? Tools for a sociology of security consumption. In: Theoretical Surveillance 14(3): 3-30

Goold, Benjamin (2009): Technologies of surveillance and the erosion of institutional trust. In: Katja Franko Aas/Helene Oppen Gundhus/Heidi Mork Lomell (Hg.): Technologies of Insecurity: The Surveillance of Everyday Life. New York: Routledge-Cavendish: 207–218

Gössner, Rolf (2002): Kollateralschäden an der „Heimatfront“. In: Ossietzky. Zweiwochenschrift für Politik/Kultur/Wirtschaft 2. Online verfügbar unter: https://www.sopos.org/aufsaetze/3c764f6821a7e/1.phtml.html [10.09.2013]

Groebner, Valentin (2004): Der Schein der Person. Steckbrief, Ausweis und Kontrolle im Mittelalter. München: C.H. Beck Verlag

Grunwald, Armin (2005): Zur Rolle von Akzeptanz und Akzeptabilität von Technik bei der Bewältigung von Technikkonflikten. In: Technikfolgenabschätzung – Theorie und Praxis 14(3): 54-60

Grusin, Richard A. (2004): Premediation. In Criticism 46(19): 17-39

Haggerty, Kevin D. (2009): ‘Ten thousand times larger …’: anticipating the expansion of sureillance. In: Benjamin J. Goold/Daniel Neyland (Hg.): New Directions in Surveillance and Privacy. Cullompton: Willan: 159-177

Haggerty, Kevin D. (2008): Tear down the walls: on demolishing the panopticon. In: David Lyon (Hg.): Theorizing Surveillance. The panopticon and beyond. Portland: Willan Publishing: 23-45

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

Hahn, Hans Peter (2004): Global Goods and the Process of Appropriation’ In: Peter Probst/Gerd Spittler (Hg.): Between Resistance and Expansion. Explorations of Local Vitality in Africa (Beiträge zur Afrikaforschung, 18). Münster: Lit: 211-229

Hardin, Russel (2001): Die Alltagsepistemologie von Vertrauen. In: Martin Hartman/Claus Offfe (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt a.M./New York: Campus: 295-332

Hartmann, Martin (2013): Zerstörtes Vertrauen, zerstörte Freiheit. Die Folgen der Überwachung aus philosophischer Sicht. In: Forschung und Lehre 20(8): 622-624

Hartmann, Martin (2011): Die Praxis des Vertrauens. Berlin: Suhrkamp Verlag

Hartmann, Martin (2002): Aussichten auf Vorteile? Grenzen rationaler Vertrauensmodelle in der Politikanalyse. In: Österreichische Zeitschrift für Politikwissenschaft 31(4): 379-395

Haug, Volker M. (2014): „Partizipationsrecht“ – Ein Plädoyer für eine eigene juristische Kategorie. In: Die Verwaltung 47(2): 221-241

Haupts, Tobias (2014): Die Videothek. Zur Geschichte und medialen Praxis einer kulturellen Institution. Bielefeld: transcript Verlag

Heesen, Jessica (2008): Keine Freiheit ohne Privatsphäre. In: Sandro Gaycken/Constanze Kurz (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: transcript Verlag: 231-248

Hempel, Leon/Susanne Krasmann/Ulrich Bröckling (2011): Sichtbarkeitsregime: Eine Einleitung. In: Diess. (Hg.): Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan. Sonderheft 25. Wiesbaden: VS Verlag für Sozialwissenschaften: 7-24

Hennen, Leonhard (1994): Ist die (deutsche) Öffentlichkeit „technikfeindlich“? Ergebnisse der Meinungs- und der Medienforschung. Erster Sachstandsbericht im Rahmen des Monitoring-Projektes „Technikakzeptanz und Kontroversen über Technik“. Arbeitsbericht Nr. 24. TAB Büro für Technikfolgenabschätzung beim Deutschen Bundestag. Online verfügbar unter: http://www.itas.kit.edu/pub/v/1994/henn94a.pdf [13.05.2014]

Henslin, James (1968): Trust and the Cab Driver. In: Marcello Truzzi (Hg.): Sociology and Everyday Life. Englewood Cliffs: Prentice-Hall: 138-157

Heritage, John (2004): Conversation analysis and institutional talk: analysing data. In: David Silverman (Hg.): Qualitative research: Theory, method and practice. London: Sage Publications: 222-245

Hermstrüver, Yoan (2016): Informationelle Selbstgefährdung. Tübingen: Mohr Siebeck

Hetzel, Andreas (2005): Technik als Vermittlung und Dispositiv: Über die vielfältige Wirksamkeit von Maschinen. In: Gerhard Gamm/Ders. (Hg.): Unbestimmtheitssignaturen der Technik. Bielefeld: transcript: 275-296

Hillebrandt, Frank (2015): Was ist der Gegenstand einer Soziologie der Praxis? In: Franka Schäfer/Anna Daniel/Ders. (Hg.): Methoden einer Soziologie der Praxis. Bielefeld: transcript Verlag: 15-36

Hillmann, Karl-Heinz (2007): Akzeptanzkrise. In: Ders. (Hg.): Wörterbuch der Soziologie. Stuttgart: Kröner Verlag: 16

Hitzler, Ronald (2009): Ethnographie. In: Buber, Renate/Hartmut H. Holzmüller (Hg.): Qualitative Marktforschung. Konzepte – Methoden – Analysen. Wiesbaden: Gabler: 207-218

Hitzler, Ronald/Miriam Gothe (2015): Zur Einleitung: Methodologisch-methodische Aspekte ethnographischer Forschungsprojekte. In: Diess. (Hg.): Ethnographische Erkundungen. Methodische Aspekte aktueller Forschungsprojekte. Wiesbaden: Springer VS: 9-16

Hopf, Christel (2005): Qualitative Interviews. Ein Überblick. In: Uwe Flick/Ernst von Kardorff/Ines Steinke (Hg.): Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg: Rowohlt: 349-360

Hopf, Christel (1991): Das qualitative Interview. In: Uwe Flick et al. (Hg.): Handbuch Qualitative Sozialforschung. München: Psychologie Verlags Union: 177-182

Honer, Anne (2003): Interview. In: Ralf Bohnsack/Winfried Marotzki/Michael Meuser (Hg): Hauptbegriffe Qualitativer Sozialforschung. Opladen: Springer VS: 94-99

Hornecker, Eva (2004): Videobasierte Interaktionsanalyse – der Blick durch die (Zeit-)Lupe auf das Interaktionsgeschehen kooperativer Arbeit. Online verfügbar unter: http://www.ehornecker.de/Papers/KOPRA_Final.pdf [13.04.2013]

Hörning, Karl H. (2001): Experten des Alltags. Die Wiederentdeckung des praktischen Wissens. Weilerstwist: Velbrück Wissenschaft

Hörning, Karl H. (1988): Technik im Alltag und die Widersprüche des Alltäglichen. In: Bernward Joerges (Hg.): Technik im Alltag. Frankfurt a.M.: Suhrkamp: 51-94

Hornung, Gerrit (2007): Reisepässe mit Biometrie und RFID-Chips – Bausteine einer Identitätsinfrastruktur? In: Nils Zurawski (Hg.): Sicherheitsdiskurse. Angst, Kontrolle und Sicherheit in einer „gefährlichen“ Welt. Frankfurt a.M.: Peter Lang: 139-158

Hornung, Gerrit (2005): Die digitale Identität, Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren. Baden-Baden: Nomos

Hornung, Gerrit (2004): Biometrische Systeme – Rechtsfragen eines Identifikationsmittels der Zukunft. In: Kritische Justiz 37(4): 344-360

Hubert, Eva (1983): Politiker fragen – Bürger antworten nicht! Die Boykottbewegung gegen die Volkszählung. In: Jürgen Taeger (Hg.): Die Volkszählung. Mit einem Streitgespräch zwischen Hans Peter Bull und Günter Grass. Reinbek bei Hamburg: Rowohlt: 254-266

Hubig, Christoph (2011): Virtualisierung der Technik – Virtualisierung der Lebenswelt. Neue Herausforderungen für eine Technikethik als Ermöglichungsethik. In: Carl F. Gethmann (Hg.): Lebenswelt und Wissenschaft. XXI. Deutscher Kongreß für Philosophie. 15.-19. September 2008 an der Universität Duisburg-Essen. Hamburg: Felix Meiner Verlag: 146-159

Huysmans, Jeff (2006): The Politics of Insecurity. Fear, migration und asylum in the EU. New York: Routledge

Inness, Julie (1992): Privacy, Intimacy and Isolation. Oxford: Oxford University Press

Introna, Lucas D./David Wood (2004): Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. In: Surveillance and Society 2(2/3): 177-198

Iser, Wolfgang (2007): Das Imaginäre: Kein isolierbares Phänomen. In: Dieter Henrich/Ders. (Hg.): Funktionen des Fiktiven (Poetik und Hermeneutik X). München: Wilhelm Fink Verlag: 479-486

Jakobs, Eva-Maria/Ortwin Renn/Peter Weingart (2009): Technik und Gesellschaft. In: Joachim Milber (Hg.): Förderung des Nachwuchses in Technik und Naturwissenschaft. Beiträge zu den zentralen Handlungsfeldern. Berlin/Heidelberg: Springer: 219-267

James, Tabitha/Taner Pirim/Katherine Boswell/Brian Riethel/Reza Barkhi (2006): Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. In: Journal of Organizational and End User Computing 18(3): 1-24

Janke, Marcus (2002): Die ‚Parkinson-Card', eine biometrische SmartCard mit integriertem Fingerprint Sensor. In: Veronika Nolde/Lothar Leger (Hg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete. Köln: Deutscher Wirtschaftsdienst: 203-212

Jaufmann, Dieter (1999): Technikakzeptanzforschung. In: Stephan Bröchler/Georg Simonis/Karsten Sundermann (Hg.): Handbuch Technikfolgenabschätzung. Band 1. Berlin: Edition Sigma: 205-225

Joerges, Bernward (1996): Technik, Körper der Gesellschaft. Arbeiten zur Techniksoziologie. Frankfurt a.M.: Suhrkamp

Jones, Karen (1996): Trust as an Affective Attitude. In: Ethics 117(1): 4-25

Katz, Cindy (2006): The State Goes Home: Local Hypervigilance of Children and the Global Retreat from Social Reproduction. In: Torin Monahan (Hg.): Surveillance and Security: Technological Politics and Power in Everyday Life. New York/Oxon: Routledge: 27-36

Kaufmann, Franz-Xaver (2012): Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften Berlin et al.: LIT

Kistler, Ernst (2005): Die Technikfeindlichkeitsdebatte – Zum politischen Missbrauch von Umfrageergebnissen. In: TATuP – Zeitschrift des ITAS für Technikfolgenabschätzung 14(3): 13-19

Klein, Inga (2011): Überwachte Sicherheit oder sichere Überwachung? Kulturelle Deutungsmuster im Diskurs um den biometrischen Reisepass. In: Nils Zurawski (Hg.): Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle. Opladen: Budrich UniPress: 87-101

Kliment, Tibor (1994): Kernkraftprotest und Medienreaktion. Deutungsmuster einer Widerstandsbewegung und öffentliche Rezeption. Wiesbaden: Deutscher Universitätsverlag

Kneer, Georg (2000): Akzeptanz von Verwaltungsentscheidungen. Ein systemtheoretischer Beitrag am Beispiel der Umweltverwaltung. In: Claudia Rademacher/Peter Wiechens (Hg.): Verstehen und Kritik. Soziologische Suchbewegungen nach dem Ende der Gewissheiten. Wiesbaden: Westdeutscher Verlag: 93-122

Knoblauch, Hubert (2002): Fokussierte Ethnographie als Teil einer soziologischen Ethnographie. Zur Klärung einiger Missverständnisse. In: Sozialer Sinn 3(1): 129-135

Knoblauch, Hubert (2001): Fokussierte Ethnographie. In: Sozialer Sinn 2(1): 123-141

Knoblauch, Hubert (2000): Frame Analysis. In: Dirk Kaesler/Ludgera Vogt (Hg.): Hauptwerke der Soziologie. Stuttgart: Kröner Verlag: 171-176

Königsdorfer, Jörg (2008): Akzeptanz von technologischen Innovationen. Nutzungsentscheidungen von Konsumenten dargestellt am Beispiel von mobilen Internetdiensten. Wiesbaden: Gabler Edition Wissenschaft

Kollmann, Tobias (1998): Akzeptanz innovativer Nutzungsgüter und -systeme. Konsequenzen für die Einführung von Telekommunikations- und Multimediasystemen. Wiesbaden: Gabler Verlag

Krasmann, Susanne (2007): The enemy on the border. Critique of a programme in favour of a preventive state. In: Punishment and society 9(3): 301-318

Krasmann, Susanne (2004): Monitoring. In: Ulrich Bröckling/Dies./Thomas Lemke (Hg.): Glossar der Gegenwart. Frankfurt a.M.: Suhrkamp: 167-173

Krasmann, Susanne (2001): Smile, you're responsible. Ein Beitrag zur Taxonomie des Neoliberalismus. In: Criminologische Vereinigung (Hg.): Retro-Perspektiven der Kriminologie. Stadt–Kriminalität–Kontrolle. Hamburg: 109-123

Krasmann, Susanne (1999): Regieren über Freiheit. Zur Analyse der Kontrollgesellschaft aus Foucaultscher Perspektive. In: Kriminologisches Journal 31(2): 107-121

Krasmann, Susanne/Reinhard Kreissl/Sylvia Kühne/Bettina Paul/Christina Schlepper (2014): Die gesellschaftliche Konstruktion von Sicherheit. Zur medialen Vermittlung und Wahrnehmung der Terrorismusbekämpfung. Schriftenreihe Sicherheit Nr. 13. Forschungsforum öffentliche Sicherheit. Berlin. Online verfügbar unter: https://www.sicherheit-forschung.de/forschungsforum/schriftenreihe_neu/sr_v_v/SchriftenreiheSicherheit_13.pdf [17.03.2017]

Krasmann, Susanne/Sylvia Kühne (2014): 'My fingerprint on Osama's cup.' On objectivity and the role of the fictive regarding the acceptance of a biometric technology. In: Surveillance & Society 12(1): 1-14.
Online verfügbar unter: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/fingerprint/osamas-cup [20.07.2018]

Krasmann, Susanne/Jan Wehrheim (2013): Biometrie. In: Rolf Gröschner/Antje Kapust/Oliver W. Lemcke (Hg.): Wörterbuch der Würde. München: Wilhelm Fink Verlag: 359-360

Kreissl, Reinhard/Heinz Steinert (2008): Für einen gesellschaftstheoretisch aufgeklärten Materialismus. In: Kriminologisches Journal 40(4): 269-283

Kühne, Sylvia (2015): Gambling with the "Gift"? On the Relationship between Security Technologies, Trust and Distrust. The Case of Fingerprinting. In: Benjamin Rampp/Martin Endress (Hg.): Trust in Times of (In-)Security. On the Relationship between the Phenomena of Security and Trust. Behemoth. A Journal of Civilisation 8(1): 24-45. Online verfügbar unter: http://ojs.ub.uni-freiburg.de/behemoth/article/view/851/817 [20.05.2017]

Kühne, Sylvia/Christina Schlepper (2018): Zur Politik der Sicherheitsversprechen: die biometrische Verheißung. In: Tobias Singelnstein/Jens Puschke (Hg.): Der Staat in der Sicherheitsgesellschaft. Schriftenreihe Staat – Souveränität – Nation. Beiträge zur aktuellen Staatsdiskussion. Wiesbaden: Springer VS: 79-99

Kühne, Sylvia/Jan Wehrheim (2013): Versicherheitlichung und Biometrie. Zur Verbreitung einer Kontrolltechnologie im Spannungsfeld von Staat, Ökonomie und Alltag. In: Daniela Klimke/Aldo Legnaro (Hg.): Politische Ökonomie und Sicherheit. Weinheim/Basel: Beltz Juventa: 303-318

Kuckartz, Udo (2010): Einführung in die computergestützte Analyse qualitativer Daten. Wiesbaden: VS Verlag für Sozialwissenshaften

Kurz, Constanze (2008): Biometrie nicht nur an den Grenzen. Erkennungsdienstliche Behandlung für jedermann. In: Sandro Gaycken/Dies. (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: transcript Verlag: 101-116

Ladwig, Bernd (2006): Freiheit. In: Gerhard Göhler/Matthias Iser/Ina Kerner (Hg.): Politische Theorie. 22 umkämpfte Begriffe zur Einführung. Wiesbaden: Springer Fachmedien: 83-100

Lagerspetz, Olli (2001): Vertrauen als geistiges Phänomen. In: Martin Hartmann/Claus Offe (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt a.M./New York: Campus: 85-113

Lahno, Bernd (2002): Der Begriff des Vertrauens. Paderborn: mentis Verlag

Lange, Hans-Jürgen (2008): Der Wandel des föderalen Sicherheitsverbundes. In: Stefan Huster/Karsten Rudolph (Hg.): Vom Rechtsstaat zum Präventionsstaat. Frankfurt a.M.: Suhrkamp: 64-81

Larson, Deborah W. (2004): Distrust: Prudent, If Not Always Wise. In: Russell Hardin (Hg.): Distrust. New York: Russell Sage Foundation: 34-59

Latour, Bruno (2010): Eine neue Soziologie für eine neue Gesellschaft. Eine Einführung in die Akteur-Netzwerk-Theorie. Berlin: Suhrkamp

Latour, Bruno (2005): Reassembling the Social. An Introduction to Actor-Network-Theory. Oxford et al.: Oxford University Press

Latour, Bruno (1996): Der Berliner Schlüssel. Erkundungen eines Liebhabers der Wissenschaften. Berlin: Akademie Verlag

Legnaro, Aldo (2011): Auf der Suche nach dem fälschungssicheren Individuum. In: Leon Hempel/Susanne Krasmann/Ulrich Bröckling (Hg.): Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Sonderheft Leviathan 25: 191-209

Legnaro, Aldo (2003): Präludium über die Kontrollgesellschaften. In: Kriminologisches Journal 35(4): 296-301

Lemke, Jay (1995): Textual Politics. Discourse and Social Dynamics. London: Taylor & Francis

Lenard, Patti Tamara (2008): Trust Your Compatriots, but Count Your Change: The Roles of Trust, Mistrust and Distrust in Democracy. In: Political Studies 56(2): 312–332

Lepsius, Oliver (2004): Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland. In: Leviathan 32(1): 64-88

Lepsius, Rainer M. (2009): Interessen, Ideen und Institutionen. Wiesbaden: VS Verlag für Sozialwissenschaften

Lepsius, Rainer M. (2004): Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland. In: Leviathan 32(1): 64-88

Lewicki, Roy J./Daniel McAllister/Robert J. Bies (1998): Trust and Distrust: New Relationships and Realities. In: The Academy of Management Review 23(3): 438-458

Lianos, Michalis/Mary Douglas (2000): Dangerization and the End of Deviance. In: David Garland/Richard Sparks (Hg.): Criminology and Social Theory. Oxford: University Press: 103-125

Linde, Hans (1982): Soziale Implikationen technischer Geräte, ihrer Entstehung und Verwendung. In: Rodrigo Jokisch (Hg.): Techniksoziologie. Frankfurt a.M.: Suhrkamp: 1-31

Lindenberg, Michael (1996): Siegeszug der Winzigkeit: Die Fingerschau der Polizei. In: Trutz von Trotha (Hg.): Politischer Wandel, Gesellschaft und Kriminalitätsdiskurs. Beiträge zur interdisziplinären wissenschaftlichen Kriminologie. Festschrift für Fritz Sack. Nomos: Baden-Baden: 283-289

Locke, John (1977): Zwei Abhandlungen über die Regierung. Herausgegeben von Walter Euchner. Frankfurt a.M.: Suhrkamp

Lodge, Juliet (2013): Nameless and Faceless: The Role of Biometrics in Realizing Quantum (In)security and (Un)accountability. In: Patrizio Campisi (Hg.): Security and Privacy in Biometrics. London: Springer: 311-337

Loftus, Bethan/Benjamin Goold (2011): Covert Surveillance and the invisibilities of policing. In: Criminology & Criminal Justice 12(3): 275-288

Lucke, Doris (1998): Riskante Annahmen – Angenommene Risiken. Eine Einführung in die Akzeptanzforschung. In: Dies./Michael Haase, Michael (Hg.): Annahme verweigert. Beiträge zur soziologischen Akzeptanzforschung. Opladen: Leske + Budrich: 15-35

Lucke, Doris (1996a): Grenzen der Legitimation. Zum Strukturwandel der Akzeptanz. In: Lars Clausen (Hg.): Gesellschaften im Umbruch: Verhandlungen des 27. Kongresses der Deutschen Gesellschaft für Soziologie. Halle a.d. Saale/Frankfurt a.M.: Campus Verlag: 473-483

Lucke, Doris (1996b): Legitimation durch Akzeptanz. Zur Subjektorientierung einer „systematischen“ Debatte. In: Zeitschrift für Rechtssoziologie 17(2): 221-248

Lucke, Doris (1995): Akzeptanz. Legitimität in der „Abstimmungsgesellschaft“. Opladen: Leske und Budrich

Lüdemann, Christian/Christina Schlepper (2013): Angst im Überwachungsstaat. Eine empirische Studie zur Akzeptanz neuer staatlicher Überwachungsmaßnahmen. In: Sandro Gaycken (Hg.): Jenseits von 1984. Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft. Bielefeld: transcript: 147-162

Lüdemann, Christian/Christina Schlepper (2011): Der überwachte Bürger zwischen Apathie und Protest. Eine empirische Studie zum Widerstand gegen staatliche Kontrolle. In: Nils Zurawski (Hg.): Überwachungspraxen. Praktiken der Überwachung und Kontrolle. Opladen: Verlag Barbara Budrich: 119-138

Lüdemann, Christian/Christina Schlepper (2010): „Willingness to Pay for Security“ bei Passagierkontrollen am Flughafen – Zu den individuellen Kosten öffentlicher Sicherheit. In: Soziale Probleme. Zeitschrift für soziale Probleme und soziale Kontrolle 21(1): 97-135

Lüders, Christian (2005): Beobachten im Feld und Ethnographie. In: Uwe Flick/Ernst von Kardorff/Ines Steinke (Hg): Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg: Rowohlt: 384-401

Lüders, Christian (2001): Teilnehmende Beobachtung. In: Ralf Bohnsack/Winfried Marotzki/Michael Meuser (Hg): Hauptbegriffe Qualitativer Sozialforschung. Opladen: Springer VS: 151-153

Luhmann, Niklas (2003): Soziologie des Risikos. Berlin: Walter de Gruyter

Luhmann, Niklas (2001): Vertrautheit, Zuversicht, Vertrauen. Probleme und Alternativen. In: Martin Hartmann/Claus Offe (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt a.M./New York: Campus: 143-160

Luhmann, Niklas (2000): Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität. Stuttgart: UTB

Luhmann, Niklas (1997): Die Moral des Risikos und das Risiko der Moral. In: Gotthard Bechmann (Hg.): Risiko und Gesellschaft. Grundlagen und Ergebnisse interdisziplinärer Risikoforschung. Opladen: Westdeutscher Verlag: 327-338

Luhmann, Niklas (1984): Soziale Systeme. Grundriß einer allgemeinen Theorie. Frankfurt a.M.: Suhrkamp

Luhmann, Niklas (1969): Legitimation durch Verfahren. Neuwied a.R./Berlin: Hermann Luchterhand Verlag GmbH

Luhmann, Niklas (1964): Funktionen und Folgen formaler Organisation. Berlin: Duncker & Humblot

Lyon, David (2007): Surveillance Studies – an overview. Cambridge/Malden: Polity Press

Lyon, David (2001): Under my skin: From Identification Papers to Body Surveillance. In: Jane Caplan/John Torpey (Hg.): Documenting Individual Identity. The development of state practices in the modern world. Princeton, Oxford: Princeton University Press: 291-310

Lyon, David/Collin J. Bennett (2008): Playing the ID card: Understanding the significance of identity card systems. In: (Diess., Hg.): Playing the Identity Card. Surveillance, security and identification in global perspective. Oxon: Routledge: 3-20

Magnet, Shoshana (2011): When Biometrics fail. Gender, Race, and the Technology of Identity. Durham/London: Duke University Press

Maltoni, Davide/Dario Maio/Anil K. Jain/Salil Prabhakar (2009): Handbook of Fingerprint Recognition. London: Springer Verlag

Mann, Steve/Jason Nolan/Barry Wellman (2003): Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. In: Surveillance & Society 1(3): 331-355. Online verfügbar unter: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3344/3306 [23.07.2015]

Manz, Ulrich (1983): Zur Einordnung der Akzeptanzforschung in das Programm sozialwissenschaftlicher Begleitforschung. Ein Beitrag zur Anwenderforschung im technischen organisatorischen Wandel. München: Verlag V. Florenz

Marcus, George E. (1995): Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography. In: Annual Review of Anthropology 24(1): 95-117

Marotzki, Winfried (2003): Leitfadeninterview. In: Ralf Bohnsack/ders./Michael Meuser (Hg): Hauptbegriffe Qualitativer Sozialforschung. Opladen: Springer VS: 114

Martin, Aaron K./Edgar A. Whitley (2013): Fixing Identity? Biometrics and the tensions of material practices. In: Media, Culture & Society 35(1): 52-60

Marx, Gary T. (2015): Coming to terms: the kaleidoscope of privacy and surveillance. In: Beate Roessler/Dorota Morkosinska (Hg.): Social Dimensions of Privacy: Interdisciplinary Perspectives. Cambridge: Cambridge University Press: 32-49

Marx, Gary T. (2006a): Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – "Hey Buddy Can You Spare a DNA?" In: Torin Monahan (Hg.): Surveillance and Security: Technological Politics and Power in Everyday Life. New York/Oxon: Routledge: 37-56

Marx, Gary T. (2006b): Forget Big Brother and Big Corporation: What about the Personal Uses of Surveillance Technology as Seen in Cases Such as Tom I. Voire? In: Rutgers Journal of Law and Urban Policy 3(4): 210-286

Marx, Gary T. (2005): Seeing Hazily (But Not Darkly) Through the Lens: Some Recent Empirical Studies of Surveillance Technologies. In: Law & Social Inquiry 30(2): 339–399

Marx, Gary T. (2003): A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. In: Journal of Social Issues 59(2): 369-390

Marx, Gary T. (2002): What's new about the "new surveillance"? Classifying for change and continuity. In: Surveillance & Society 1(1): 9-29. Online verfügbar unter: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3391/3354 [04.03.2013]

Marx, Gary T. (1988): Undercover: Police Surveillance in America. Berkeley: University of California Press

Marx, Gary T./Glenn W. Muschert (2007): Personal Information, Borders, and the New Surveillance. In: Annual Review of Law and Social Science 3: 375-395

Massumi, Brian (2010): The Future Birth of the Affective Fact. The Political Ontology of Threat. In: Melissa Gregg/Gregory J. Seigworth (Hg.): The Affect Theory Reader. Durham/London: Duke University Press: 52-70

Mattern, Friedemann (2003): Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Ders. (Hg.): Total vernetzt. Szenarien einer informatisierten Welt. Berlin/Heidelberg: Springer Verlag: 1-41

Mauss, Marcel (1990): Die Gabe. Form und Funktion des Austauschs in archaischen Gesellschaften. Frankfurt a.M.: Suhrkamp

McCahill, Michael/Finn, Rachel L. (2014): Surveillance, Capital and Resistance. Theorizing the surveillance subject. London/New York: Routledge

McNeill, Daniel (2003): Das Gesicht. Eine Kulturgeschichte. Wien: Random House

Meinefeld, Werner (2005): Hypothesen und Vorwissen in der qualitativen Sozialforschung. In: Uwe Flick/Ernst von Kardorff/Ines Steinke (Hg): Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg: Rowohlt: 265-275

Meinefeld, Werner (1977): Einstellung und soziales Handeln. Reinbek bei Hamburg: Rowohlt-Taschenbuch Verl. Sozialwissenschaft

Meintjes-Van der Walt, Lirieka (2006): Fingerprint evidence: probing myth and reality. In: South African Journal of Criminal Justice 19(2): 152-172

Meßner, Daniel (2015): Die Erfindung der Biometrie – Identifizierungstechniken und ihre Anwendungen, 1870-1914. Dissertation Universität Wien. Online verfügbar unter: http://othes.univie.ac.at/39278/1/2015-07-21_0303769.pdf [10.03.2017]

Meßner, Daniel (2010): Volksdaktyloskopie: Das Fingerabdruckverfahren als Überwachungsphantasie zwischen Ausweitung und Widerstand. In: JIPSS: 7-19

Mey, Günter/Katja Mruck (2007): Qualitative Interviews. In: Gabriele Naderer/Eva Balzer (Hg.): Qualitative Marktforschung in Theorie und Praxis: Grundlagen, Methoden und Anwendungen. Wiesbaden: Springer VS: 249-278

Misztal, Barbara A. (2001): Normality and Trust in Goffman's Theory of Interaction Order. In: Sociological Theory 19(3): 312-324

Möllering, Guido (2006): Trust: Reason, Routine, Reflexivity. Oxford: Elsevier

Möllering, Guido (2007): Grundlagen des Vertrauens: Wissenschaftliche Fundierung eines Alltagsproblems. In: Max-Planck-Institut für Gesellschaftsforschung (Hg.): Jahrbuch 2007-2008: 73-78. Online verfügbar unter: www.mpifg.de/pu/ueber_mpifg/mpifg_jb/JB0708/MPIfG_07-08.pdf [25.10.2013]

Monahan, Torin (2010): Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance. In: Kevin D. Haggerty/Minas Samatas (Hg.): Surveillance and Democracy. New York: Routledge: 91-110

Monahan, Torin (2006): The Surveillance Curriculum - Risk Management and Social Control in the Neoliberal School. In: Dies. (Hg.): Surveillance and Security: Technological Politics and Power in Everyday Life. New York/Oxon: Routledge: 109-124

Mordini, Emilio (2009): Ethics and Policy of Biometrics. In: Massimo Tistarello/Stan Z. Li/Rama Chellappa (Hg.): Handbook of Remote Biometrics for Surveillance and Security. Dordrecht/Heidelberg/London/New York: Springer: 293-309

Moses, Kenneth R. et al. (2011): Automated Fingerprint Identification System (AFIS). In: U.S. Department of Justice Office of Justice Programs (Hg.): The Fingerprint Sourcebook. Rockville: Kapitel 6

Muller, Benjamin J. (2011): Risking it all at the Biometric Border: Mobility, Limits, and the Persistence of Securitisation. In: Geopolitics 16(1): 91-106

Muller, Benjamin J. (2010): Security, Risk and the Biometric State. Oxon: Routledge

Muller, Benjamin J. (2008): Securing the Political Imagination: Popular Culture, the Security Dispositif and the Biometric State. In Security Dialogue 39(2-3): 199-220

Muller, Benjamin J. (2004): (Dis)qualified bodies: securitization, citizenship and 'identity management'. In: Citizenship Studies 8(3): 279-294

Murakami-Wood, David (2011): Vanishing Surveillance: Why Seeing What is Watching Us Matters. Online verfügbar unter: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/wood_201107/ [16.01.2013]

Murakami-Wood, David et al. (2006): A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network. Online verfügbar unter: https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf [14.03.2011]

Murakami-Wood, David/C. William R. Webster (2009): Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example. In: Journal of Contemporary European Research 5(2): 259-273

Murray, Harry (2000): Deniable Degradation: The Finger-Imaging of Welfare Recipients. In: Sociological Forum 15(1): 39-63

Murray, Heather (2007): Monstrous Play in Negative Spaces: Illegible Bodies and the Cultural Construction of Biometric Technology. In: The Communication Review 10(4): 347-365

Nayar, Pramod K. (2015): Citizenship and Identity in the age of surveillance. Cambridge: Cambridge University Press

Nettesheim, Martin (2010): Erster Beratungsgegenstand: Grundrechtsschutz der Privatheit. In: Ders. et al. (Hg.): Der Schutzauftrag des Rechts. Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010. Berlin: De Gruyter: 7-49

Neyland, Daniel (2009): Who's Who? The Biometric Future and the Politics of Identity. In: European Journal of Criminology 6(2): 135-155

Ng-Kruelle, Grace/Paul A. Swatman/J. Felix Hampe/Douglas S. Rebne (2006): Biometrics and e-Identity (e-Passport) in the European Union: End-user perspectives on the adoption of a controversial innovation. In: Journal of Theoretical and Applied Electronic Commerce Research 1(2): 12-35

Nissenbaum, Helen (2011): Privatsphäre im Kontext: Technologie, Politik und die Unversehrtheit des Sozialen. In: Heinrich-Böll-Stiftung (Hg.): #public_life. Digitale Intimität, die Privatsphäre und das Netz. Berlin: 53-63. Online verfügbar unter: https://www.boell.de/sites/default/files/2011-04-public_life.pdf [14.05.2017]

Nissenbaum, Helen (2004): Privacy as contextual integrity. In: Washington Law Review 79: 101-139

Nogala, Detlef (2000): Gating the Rich – Barcoding the Poor: Konturen einer neoliberalen Sicherheitskonfiguration. In: Wolfgang Ludwig-Mayerhofer (Hg.): Soziale Ungleichheit, Kriminalität und Kriminalisierung. Opladen: Leske + Budrich: 49-83

O'Malley, Pat (2004): Risk, Uncertainty and Government. London: Glasshouse

Offe, Claus (2001): Können wir unseren Mitbürgern vertrauen? In: Martin Hartmann/Ders. (Hg.): Vertrauen. Die Grundlage des sozialen Zusammenhalts. Frankfurt a.M./New York: Campus: 241-294

Oldemeyer, Ernst (1988): Wertkonflikte um die Technikakzeptanz. In: Walter Bungard/Hans Lenk (Hg.): Technikbewertung. Frankfurt a.M.: Suhrkamp: 33-45

Opitz, Sven (2014): Zur Soziologie der Affekte: Resonanzen epidemischer Angst. In: Joachim Fischer/Stephan Moebius (Hg.): Kultursoziologie im 21. Jahrhundert. Wiesbaden: Springer Fachmedien: 269-284

Osterloh, Margit/Antoinette Weibel (2006): Vertrauen – ein schillernder Begriff. In: Diess. (Hg.): Investition Vertrauen. Prozesse der Vertrauensentwicklung in Organisationen. Wiesbaden: Gabler Verlag: 33-70

Paulus, Sachar (2011): Interview mit Sachar Paulus. In: Hempel, Leon/Susanne Krasmann/Ulrich Bröckling (2011): Sichtbarkeitsregime: Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan. Sonderheft 25. Wiesbaden: VS Verlag für Sozialwissenschaften: 143-154

Petermann, Thomas (2010): Biometrie als globale Kontrolltechnologie: Die Rolle der Technikfolgenabschätzung. In: Marion Albers/Ruth Weinzierl (Hg.): Menschenrechtliche Standards in der Sicherheitspolitik. Baden-Baden: Nomos: 129-145

Petermann, Thomas (1999): Einführung: Technikfolgen-Abschätzung – Konstituierung und Ausdifferenzierung eines Leitbilds. In: Stephan Bröchler/Georg Simonis/Karsten Sundermann (Hg.): Handbuch Technikfolgenabschätzung. Bd. 1. Berlin: Edition Sigma: 17-49

Petermann, Thomas/Arnold Sauter (2002): Biometrische Identifikationssysteme. Sachstandsbericht. Büro für Technikfolgenabschätzung beim Deutschen Bundestag. Arbeitsbericht Nr. 76. Online verfügbar unter: http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab076.pdf [14.04.2013]

Petermann, Thomas/Constanze Scherz (2005): TA und (Technik-)Akzeptanz(-forschung). In: Technikfolgenabschätzung – Theorie und Praxis 14(3): 45-53

Pethes, Nicolas (2004): EDV im Orwellstaat. Der Diskurs über Lauschangriff, Datenschutz und Rasterfahndung um 1984. In: Irmela Schneider/Christina Bartz/Isabell Otto (Hg.): Medienkultur der 70er Jahre. Diskursgeschichte der Medien nach 1945. Band 3. Wiesbaden: VS Verlag für Sozialwissenschaften: 57-75

Pfeifer, Wolfgang et al. (1993): Requisit. In: Etymologisches Wörterbuch des Deutschen (1993): Digitalisierte und von Wolfgang Pfeifer überarbeitete Version im Digitalen Wörterbuch der deutschen Sprache. Online verfügbar unter: https://www.dwds.de/wb/Requisit [15.09.2015]

Pfitzmann, Andreas (2005): Biometrie – wie einsetzen und wie keinesfalls? Wie umgehen mit Sicherheitsproblemen von Biometrie und Sicherheits- und Datenschutzproblemen durch Biometrie? Online verfügbar unter: http://www.inf.tu-dresden.de/index.php?node_id=703 [12.05.2013]

Pietsch, Carsten/Rüdiger Fiebig (2011): „Keine besondere Bedrohungslage“: Die Einstellungen der deutschen Bevölkerung zu Maßnahmen der Terrorabwehr. In: Thomas Jäger (Hg.): Die Welt nach 9/11. Wiesbaden: VS Verlag für Sozialwissenschaften: 261-284

Pinch, Trevor J./Wiebe E. Bijker (1984): The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. In: Social Studies of Science 14(3): 399-441

Prainsack, Barbara/Martin Kitzberger (2009): Other Ways of Knowing Forensic DNA Technologies. In: Social Studies of Science 39(1): 52-79

Prantl, Heribert (2002): Verdächtig. Der starke Staat und die Politik der inneren Unsicherheit. Hamburg: Europa Verlag

Preisendörfer, Peter (1995): Vertrauen als soziologische Kategorie. Möglichkeiten und Grenzen einer entscheidungstheoretischen Fundierung des Vertrauenskonzepts. In: Zeitschrift für Soziologie 24(4): 263-272

Probst, Thomas (2002): Biometrie aus datenschutzrechtlicher Sicht. In: Veronika Nolde/Lothar Leger (Hg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete. Köln: Deutscher Wirtschaftsdienst: 115-128

Pugliese, Joseph (2010): Biometrics, Bodies, Technologies, Biopolitics. New York, Oxon: Routledge

Rammert, Werner (2007): Technik – Handeln – Wissen. Zu einer pragmatistischen Technik- und Sozialtheorie. Wiesbaden: VS Verlag für Sozialwissenschaften

Rammert, Werner (2007b): Technografie trifft Theorie. Forschungsperspektiven einer Soziologie der Technik. Technical University Technology Studies. Working Papers 1-2007. Online verfügbar unter: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-12091 [20.04.2013]

Rammert, Werner (1999): Technik. Stichwort für eine Enzyklopädie. Technical University Technology Studies. Working Papers 1-1999. Online verfügbar unter: http://nbn-resolving.de/urn:nbn:de:0168-ssoar-8811 [20.04.2013].

Rammert, Werner (1988): Technisierung im Alltag. In: Bernhard Joerges (Hg.): Technik im Alltag. Frankfurt a.M.: Suhrkamp: 165-197

Rammert, Werner/Ingo Schulz-Schaeffer (2002): Technik und Handeln. Wenn soziales Handeln sich auf menschliches Verhalten und technische Abläufe verteilt. In: Diess. (Hg.): Können Maschinen handeln? Soziologische Beiträge zum Verhältnis von Mensch und Technik. Frankfurt a.M./New York: Campus Verlag: 11-64

Reckwitz, Andreas (2003): Grundelemente einer Theorie sozialer Praktiken. Eine sozialtheoretische Perspektive. In: Zeitschrift für Soziologie 32(4): 282-301

Regener, Susanne (1999): Fotografische Erfassung. Zur Geschichte medialer Konstruktionen des Kriminellen. München: Fink

Reichertz, Jo (2014): Von Menschen und Dingen. Wer handelt hier eigentlich? In: Angelika Poferl/Norbert Schröer (Hg.): Wer oder was handelt? Zum Subjektverständnis der hermeneutischen Wissenssoziologie. Wiesbaden: Springer Fachmedien: 95-120

Reinhold, Gerd/Siegfried Lamnek/Helga Recker (2001): Akzeptanzkrise. In: Diess. (Hg.): Soziologie-Lexikon. München/Wien: Oldenbourg: 11

Renn, Ortwin (2010): Sicherheit, Risiko und Vertrauen. In: Petra Winzer/Eckehard Schnieder/Friedrich-Wilhelm Bach (Hg.): Sicherheitsforschung: Chancen und Perspektiven. Acatech - Deutsche Akademie der Technikwissenschaften. Berlin/Heidelberg: Springer Verlag: 163-183

Renn, Ortwin (2005): Technikakzeptanz: Lehren und Rückschlüsse der Akzeptanzforschung für die Bewältigung des technischen Wandelns. In: Technikfolgenabschätzung – Theorie und Praxis 14(3): 29-38

Renn, Ortwin (1993): Technik und gesellschaftliche Akzeptanz Herausforderungen der Technikfolgenabschätzung. In: GAIA 2(2): 67-83

Renn, Ortwin (1991): Risikokommunikation: In: Jörg Schneider (Hg.): Risiko und Sicherheit technischer Systeme. Auf der Suche nach neuen Ansätzen. Basel: Birkhäuser Verlag: 193-209

Renn, Ortwin (1986): Akzeptanzforschung. Technik in der gesellschaftlichen Auseinandersetzung. In: Chemie in unserer Zeit 20(2): 44-52

Renn, Ortwin/Michael M. Zwick (1997): Risiko- und Technikakzeptanz. Berlin et al.: Springer

Rischmüller, Frauke (2012): Gabe und Vertrauen. Eine französische Perspektive. In: Annette Schnabel/Rainer Schützeichel (Hg.): Emotionen, Sozialstruktur und Moderne. Wiesbaden: Springer VS: 299-315

Rogers, Everett M. (2003): Diffusion of Innovation. New York: Free Press

Ropohl, Günter (2010): Das Misstrauen in der Technikdebatte. In: Matthias Maring (Hg.): Vertrauen – Zwischen sozialem Kitt und der Senkung von Transaktionskosten. Karlsruhe: KIT Scientific Publishing: 115-132

Ross, Arun/Jidnya Shah/Anil K. Jain (2007): From Template to Image: Reconstructing Fingerprints from Minutiae Points. In: IEEE Transaction on Pattern Analysis and Machine Intelligence 29(4): 544-560

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

Roßler, Gustav (2016): Der Anteil der Dinge an der Gesellschaft. Sozialität – Kognition – Netzwerke. Bielefeld: transcript Verlag

Saborowski, Maxine (2008): Die Biodaten des Menschen. Der ‚Wert' der unbegrenzten Möglichkeiten. In: Leviathan 36(1): 85-104

Sarkar, Swagato (2014): The Unique Identity (UID) Project, Biometrics and Re-Imagining Governance in India. In: Oxford Development Studies 42(4): 516-533

Schaar, Peter (2010): Sicherheit und Freiheit brauchen Datenschutz. In: Bundeszentrale für Politische Bildung. 22.11.2010. Online verfügbar unter: http://www.bpb.de/internationales/europa/europa-kontrovers/38193/standpunkt-peter-schaar?p=all [15.06.2005]

Schäfer, Martina/Dorothee Keppler (2013): Modelle der technikorientierten Akzeptanzforschung. Überblick und Reflexion am Beispiel eines Forschungsprojekts zur Implementierung innovativer technischer Energieeffizienz-Maßnahmen. discussion paper 34. Berlin: Technische Universität Berlin. Online verfügbar unter: https://www.tu-berlin.de/fileadmin/f27/PDFs/Discussion_Papers_neu/discussion_paper_Nr__34.pdf [27.03.2014]

Schlepper, Christina/Christina Wickert/Judith Wöbcke/Bettina Paul (2015): „… das kennt man ja vom Flughafen". Über die Akzeptanz neuer Sicherheitsmaßnahmen im Fährverkehr. In: Gerrit Herlyn/Nils Zurawski (Hg.): Achtung Sicherheitskontrollen! Flughäfen, Kultur, Un/Sicherheiten. Münster: Lit-Verlag: 191-215

Schulz-Schaeffer, Ingo (2000): Sozialtheorie der Technik. Frankfurt a.M.: Campus-Verlag

Schütz, Alfred (2004): Der sinnhafte Aufbau der sozialen Welt. Eine Einleitung in die verstehende Soziologie. Frankfurt a.M.: Suhrkamp

Schütz, Alfred (1972): Gesammelte Aufsätze Band 2. Herausgegeben von Arvid Brodersen. Den Haag: Martinus Nijhoff

Schütz, Alfred/Peter Luckmann (2003): Strukturen der Lebenswelt. Konstanz: UVK Verlagsgesellschaft

Scott, James (1998): Seeing like a State: How certain Schemes to Improve the Human Condition Have Failed. Durham: Yale University Press

Sengoopta, Chandak (2003): Imprint of the Raj: How Fingerprinting Was Born in Colonial India. London: Pan

Siegrist, Michael (2001): Die Bedeutung von Vertrauen bei der Wahrnehmung und Bewertung von Risiken. Arbeitsbericht Nr. 197 der Akademie für Technikfolgenabschätzung in Baden-Württemberg. Stuttgart. Online verfügbar unter: https://d-nb.info/1025256190/34 [15.06.2016]

Siemoneit, Oliver (2007): Context-Awareness und rationale Risikowahrnehmung. In: Rainer Koschke et al. (Hg.): Informatik 2007. Informatik trifft Logistik. Band 1. Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e.V. (GI). 24.-27.September 2007 in Bremen: 349-353. Online verfügbar unter: http://subs.emis.de/LNI/Proceedings/Proceedings109/gi-proc-109-064.pdf [10.03.2013]

Simmel, Georg (1992): Soziologie. Untersuchungen über die Formen der Vergesellschaftung. Gesamtausgabe Band 11. Frankfurt a.M.: Suhrkamp

Simmel, Georg (1989): Philosophie des Geldes. Gesamtausgabe Band 6. Frankfurt a.M.: Suhrkamp

Singelnstein, Tobias/Peer Stolle (2006): Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert. Wiesbaden: VS Verlag für Sozialwissenschaften

Slater, Candace (2003): In Search for the Rain Forest. In: Dies. (Hg.): In Search for the Rain Forest. North Carolina: Duke University Press: 3-40

Spieß, Christian Heinrich (1966): Der gläserne Ökonom. Das ist: Die Geschichte von Jakob W***r. In: Ders.: Biographien der Wahnsinnigen. Herausgegeben von Wolfgang Promies. Neuwied/Berlin: Hermann Luchterhand GmbH: 44-61

Spreen, Dierk (2010): Die Sicherheit der Weltgesellschaft. In: Axel Groenemeyer (Hg.): Wege der Sicherheitsgesellschaft. Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten. Wiesbaden: VS Verlag für Sozialwissenschaften: 192-229

Steeves, Valerie/Owain Jones (2010): Surveillance, children and childhood. In: Surveillance & Society 7(3/4): 187-191. Online verfügbar unter: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4151/4154 [30.06.2013]

Steuble, Annette (1983): Zur Integration von nonverbaler Kommunikation (NVK) in die Gesprächsanalyse – exemplarische Analyse eines Prüfungsgesprächs. In: Gisbert Keseling/Arne Wrobel (Hg.): Latente Gesprächsstrukturen. Untersuchungen zum Problem der Verständigung in Psychotherapie und Pädagogik. Weinheim/Basel: Beltz: 175-231

Strack, Fritz/Petra Markel (2013): Abschlussbericht Verbundprojekt: MuViT. Mustererkennung und Video Tracking: sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen. Teilprojekt: MuViT – SozPsy Exposition und Akzeptanz - Sozialpsychologische Studien in Reaktion auf Mustererkennung und Video Tracking. Universität Tübingen. Online verfügbar unter: https://www.tib.eu/suchen/id/TIBKAT:819647292/ [14.03.2017]

Strasser, Peter (2006): Biometrie – ein Schritt in die Überwachungsdemokratie? In: Peter Schaar (Hg.): Biometrie und Datenschutz – Der vermessene Mensch. Tagungsband zum Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 27. Juni 2006 in Berlin. Bonn: 11-25.

Strasser, Peter (2005): Verbrechermenschen. Zur kriminalwissenschaftlichen Erzeugung des Bösen. Frankfurt a.M.: Campus-Verlag

Strauss, Anselm L. (2004): Methodologische Grundlagen der Grounded Theory. In: Jörg Strübing/Bernd Schnettler (Hg.): Methodologie interpretativer Sozialforschung: Klassische Grundlagentexte. Konstanz: UVK: 429-451

Strauss, Anselm L./Juliet Corbin (1996): Grounded Theory. Grundlagen Qualitativer Sozialforschung. Weinheim: Beltz/Psychologie Verlagsunion

Strickland, Lloyd H. (1958): Surveillance and Trust. In: Journal of Personality 26(2): 200-215

Strübing, Jörg (2008): Grounded Theory. Zur sozialtheoretischen und epistemologischen Fundierung des Verfahrens der empirisch begründeten Theoriebildung. Wiesbaden: VS Verlag für Sozialwissenschaften

Suchman, Lucy A. (1985): Plans and situated actions. The problem of human-machine communication. Palo Alto: Xerox

Sztompka, Piotr (1998): Trust, Distrust and Two Paradoxes of Democracy. In: European Journal of Social Theory 1(1): 19-32

Thomas, William I./Dorothy Swaine Thomas (1970): The child in America: behavior problems and programs. New York: Knopf

Traut, Andreas/Michale Nagenborg/Benjamin Rampp/Regina Ammich Quinn (2010): Körperscanner – Sicherheiten und Unsicherheiten. In: forum kriminalprävention 1: 14-20.

Tschida, Ulla (2014): Auf der Suche nach dem Artefakt. Zur materiellen Praxis von Infrastruktur-Entwicklung. In: Friederike Elias/Albrecht Franz/Henning Murmann/Ulrich Wilhelm Weiser (Hg.): Praxeologie. Beiträge zur interdisziplinären Reichweite praxistheoretischer Ansätze in den Geistes- und Sozialwissenschaften. Berlin/Boston: De Gruyter: 219-242

Tyler, Tom R. (2006): Viewing CSI and the Threshold of Guilt: Managing Truth and Justice in Reality and Fiction. In: The Yale Law Journal 115(5): 1050-1085

Tyler, Tom (1998): Trust and Democratic Governance. In: Valerie Braithwaite/Margaret Levi (Hg.): Trust and Governance. New York: Russel Sage Foundation: 269-294

Ullrich, Carsten G. (2008): Die Akzeptanz des Wohlfahrtsstaates. Präferenzen, Konflikte, Deutungsmuster. Wiesbaden: VS Verlag für Sozialwissenschaften

van der Ploeg, Irma (2003a): Biometrics and Privacy. A note on the politics of theorizing technology. In: Information, Communication & Society 6(1): 85-104

van der Ploeg, Irma (2003b): Biometrics, and the body as information: Normative issues of the socio-technical coding of the body. In: David Lyon (Hg.): Surveillance and social sorting. Privacy, risk and digital discrimination. London/New York: Routledge: 57-73

van der Ploeg, Irma (1999a): Written on the body: Biometrics and Identity. In: Computers and Society 29(1): 37–44.

van der Ploeg, Irma (1999b): The illegal body: 'Eurodac' and the politics of biometric identification. In: Ethics and Information Technology 1(4): 295-302

Vasilache, Andreas (2012): Sicherheit, Entgrenzung und die Suspendierung des Privaten. In: Christopher Daase/Philipp Offermann/Valentin Rauer (Hg.): Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr. Frankfurt a.M.: Campus: 133-135

Vec, Miloš (2002): Die Spur des Täters: Methoden der Identifikation in der Kriminalistik (1879-1933). Baden-Baden: Nomos-Verlags-Gesellschaft

Venkatesh, Viswanath/Fred D. Davis (2000): A theoretical extension of the technology acceptance model: four longitudinal field studies. In: Management Science 46(2): 186-204

Vester, Heinz-Günter (2009): Kompendium der Soziologie I: Grundbegriffe. Wiesbaden: VS Verlag für Sozialwissenschaften

Wagner, Gerald (1994): Vertrauen in Technik. In: Zeitschrift für Soziologie 23(2): 145-157

Walby, Kevin T. (2005): Institutional Ethnography and Surveillance Studies: An Outline for Inquiry. In: Surveillance & Society 3(2/3): 158-172. Online verfügbar unter: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3498/3452 [30.06.2016]

Weber, Maik (2008): Akzeptanz biometrischer Authentifizierungssysteme. Dissertation Univ. Mannheim. Mannheim

Weber, Max (1972): Wirtschaft und Gesellschaft. Tübingen: Mohr Siebeck

Weltecke, Dorothea (2003): Gab es „Vertrauen" im Mittelalter? Methodische Überlegungen. In: Ute Frevert (Hg.): Vertrauen. Historische Annäherungen. Göttingen: Vandenhoeck & Ruprecht: 7-66

Wiedemann, Peter M./Johannes Mertens (2005): Sozialpsychologische Risikoforschung. In: Technikfolgenabschätzung – Theorie und Praxis 14(3): 38-45

Wiener, Norbert (1989): The Human Use of Human Beings: Cybernetics and Society. London: Free Association Books

Winner, Langdon (1980): Do Artifacts Have Politics? In: Daedalus 109(1): 121-136

Witzel, Andreas (2000): Das problemzentrierte Interview. In: Forum Qualitative Sozialforschung 1(1). Art. 22. Online verfügbar unter: http://www.qualitative-research.net/index.php/fqs/article/view/1132 [17.05.2017]

Witzel, Andreas (1985): Das problemzentrierte Interview. In: Gerd Jüttemann (Hg.): Qualitative Forschung in der Psychologie: Grundfragen, Verfahrensweisen, Anwendungsfelder. Weinheim/Basel: Beltz Verlag: 227-255

Würtenberger, Thomas (1996): Die Akzeptanz von Verwaltungsentscheidungen. Baden-Baden: Nomos Verlag

Würtenberger, Thomas/Steffen Tanneberger (2010): Gesellschaftliche Voraussetzungen und Folgen der Technisierung von Sicherheit. In: Petra Winzer/Eckehard Schnieder/Friedrich-Wilhelm Bach (Hg.): Sicherheitsforschung: Chancen und Perspektiven. Acatech - Deutsche Akademie der Technikwissenschaften. Berlin/ Heidelberg: Springer Verlag: 221-240

Yar, Majid (2003): Panoptic Power and the Pathologisation of Vision: Critical Reflections on the Foucauldian Thesis. In: Surveillance & Society 1(3): 254-271. Online verfügbar unter: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3340Z [16.04.2013]

Zurawski, Nils (2011): Local Practice and Global Data: Loyalty Cards, Social Practices, and Consumer Surveillance. In: The Sociological Quarterly 52: 509-527

Zurawski, Nils (2007): Einleitung: Von Unsicherheit, Angst und Gegenmaßnahme. In: Ders. (Hg.): Sicherheitsdiskurse. Angst, Kontrolle und Sicherheit in einer „gefährlichen“ Welt. Frankfurt a.M.: Peter Lang: 9-18

Zureik, Elia (2010): Surveillance, privacy, and the globalization of personal information: international comparisons. Montréal, Québec: McGill-Queen

Quellen

Bitkom (2009a): Biometrie aus Deutschland weltweit führend. Presseinformation vom 3. September 2009. Online verfügbar unter: http://www.bitkom.org/61330_60912.aspx [09.08.2011]

Bitkom (2009b): Biometrie. Referenzprojekte. 2. Auflage. Berlin.

Bitkom (2007): Zukunft digitale Wirtschaft. Gemeinsame Studie des BITKOM e. V. und der Roland Berger Strategy Consultants. Berlin. Online verfügbar unter: https://www.bitkom.org/Bitkom/Publikationen/Zukunft-digitale-Wirtschaft.html [14.03.2018]

Bitkom (2005): Elektronischer Reisepass ist eine Chance für die deutsche Sicherheitswirtschaft. Online verfügbar unter: https://bitkom.org/files/documents/BITKOM_PI_Elektronischer_Reisepass_04.10.205.pdf [22.06.2013]

Böger, Jana (2012): Biometrie als Sicherheits- oder Lifestyle-Technologie? Darstellungen der biometrischen Fingerabdruck-Technik: Perspektiven, Motive und Folgen. Unveröffentlichte Masterarbeit. Universität Hamburg, Fakultät für Wirtschafts- und Sozialwissenschaften

BR-Drs. 920/1/01 (22.11.2001): Empfehlungen der Ausschüsse der 770. Sitzung des Bundesrates am 30.11.2001. Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus

BT-Drs. 16/5507 (29.05.2007): Antwort der Bundesregierung auf Anfrage Drs: 16/5228 (Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen)

BT-Drs. 15/4000 (21.10.2004): Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (17. Ausschuss) gemäß § 56a der Geschäftsordnung. Technikfolgenabschätzung. Hier: TA-Projekt: Biometrie und Ausweisdokumente – Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zweiter Sachstandsbericht

BT-Drs. 14/10005 (10.10.2002): Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (19. Ausschuss) gemäß §56a der Geschäftsordnung. Technikfolgenabschätzung. Hier: TA-Projekt: Biometrische Identifikationssysteme – Sachstandsbericht

BT-Drs. 920/01 (08.11.2001): Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz)

BT-Drs. 14/1405 (14.07.1999): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Angela Marquardt, Dr. Heinrich Fink und der Fraktion der PDS - Drucksache 14/1226 - Förderung biometrischer Verfahren und ihrer datenschutzrechtlichen Begleitung durch die Bundesregierung

BT-Protokoll 16/100 (24.05.2007): Stenographischer Bericht der 100. Sitzung der 16. Wahlperiode

BT-Protokoll 16/79 (01.02.2007): Stenographischer Bericht der 79. Sitzung der 16. Wahlperiode

BT-Protokoll 15/129 (30.09.2004): Stenografischer Bericht 129. Sitzung der 15. Wahlperiode

BT-Protokoll 14/209 (14.12.2001): Stenographischer Bericht der 209. Sitzung der 14. Wahlperiode

BT-Protokoll 14/192 (01.10.2001): Stenographischer Bericht der 192. Sitzung der 14. Wahlperiode

Bundesamt für Sicherheit in der Informationstechnik (2003): BioFace. Vergleichende Untersuchung von Gesichtserkennungssystemen. Öffentlicher Abschlussbericht BioFace I & II, Bonn. Online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFace/BioFaceIIBericht.pdf?__blob=publicationFile&v=4 [16.07. 2016]

Bundesamt für Sicherheit in der Informationstechnik (o.J.a): Fingerabdruckerkennung. Online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Fingerabdruckerkennung_pdf.pdf?__blob=publicationFile [16.08.2014]

Bundesamt für Sicherheit in der Informationstechnologie (o.J.b): Einführung in die technischen Grundlagen der biometrischen Authentisierung. Online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.html [15.06.2015]

Bundesministerium des Innern (2010): Alles Wissenswerte zum neuen Personalausweis. Berlin. Online verfügbar unter: https://www.personalausweisportal.de/SharedDocs/Downloads/Pressemappe/PersonalausweisbroschuereA6.pdf?__blob=publicationFile [14.02.2014]

Bundesministerium des Innern (2007): Der elektronische Reisepass – Informationsfilm. Berlin. Online verfügbar unter: https://www.youtube.com/watch?v=K5rdzZhuXDc [13.05. 2017]

Chaos Computer Club (2008): Basteltipps Biometrieversand. In: Die Datenschleuder 92: 56-57. Online verfügbar unter: http://ds.ccc.de/pdfs/ds092.pdf [15.06.2013]

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2011): Biometrische Merkmale bei Visa und Aufenthaltserlaubnissen von Ausländern zur Einreise in einen ‚Schengen-Staat'. Online verfügbar unter: http://www.bfdi.bund.de/cln_029/nn_533592/DE/Schwerpunkte/Biometrie/Artikel/BiometrischeMerkmaleSchengen.html [12.08.2011]

Der Spiegel (13.02.1978): Gläserner Mensch: 32-33.

European Commission (2005a): Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs. Brussels. 24.11.2005. COM (2005) 597 final. Online verfügbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF [19.8.2011]

European Commission (2005b): Biometrics at the Frontiers: Assessing the Impact on SocietyFor the European ParliamentCommittee on Citizens' Freedoms and Rights,Justice and Home Affairs (LIBE). Online verfügbar unter: http://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf [14.05.2017]

European Council (2003): Thessaloniki European Council 19 and 20 june 2003. Presidency Conclusions. Brussels, 1 October 2003. Online verfügbar unter: http://ue.eu.int/ueDocs/cms_Data/docs/pressdata/en/ec/76279.pdf [19.08.2011]

Gellman, Barton/Laura Poitras (2013): U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. In: The Washington Post. 07.06.2013. Online verfügbar unter: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1 [25.06.2013]

Greenwald, Glenn/Ewen MacAskill (2013): NSA Prism program taps into user data of Apple, Google and others. In: The Guardian. 07.06.2013. Online verfügbar unter: http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data [25.06.2013]

Herzinger, Richard (2003): Die Freiheit nehm ich dir. Der Bürger wird rundum überwacht und findet nichts dabei. In: Zeit Online (31.07.2001): Online verfügbar unter: http://www.zeit.de/2003/32/01___Leiter_1 [15.06.2016]

Medina, Miriam (2010): "Hey Brother Can You Spare a Dime?" Part III The Decade of the Thirties: The Effects of the Great Depression. Online verfügbar unter: http://www.thehistorybox.com/your_the_writer/article_16e.html [14.06.2015]

New York Times (17.12.2001): Technology & Media: A Surge in Demand To Use Biometrics. Online verfügbar unter: http://www.nytimes.com/2001/12/17/business/technology-media-a-surge-in-demand-to-use-biometrics.html. [22.07.2016]

Prantl, Heribert (2012): Polizei soll Zugriff auf Fingerabdrücke erhalten. Süddeutsche Zeitung 17. Dezember 2012. Online verfügbar unter: http://www.sueddeutsche.de/politik/daten-von-fluechtlingen-in-der-eu-polizei-soll-zugriff-auf-fingerabdruecke-erhalten-1.1552542 [15.06.2013]

Schaar, Peter (2009): Vorwort. In: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Hg.): 25 Jahre Volkszählungsurteil. Datenschutz – Durchstarten in die Zukunft! Festveranstaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus Anlass des 25. Jahrestages der Verkündung des Volkszählungsurteils des Bundesverfassungsgerichts am 15. Dezember 2008 im Bürgersaal des Karlsruher Rathauses. Dokumentation. Berlin: 5-6: Online verfügbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/Tagungsbaende/Dokumentation25JahreVolkszaehlungsurteil.pdf?__blob=publicationFile&v=5 [14.06.2015]

Schily, Otto (2001): ‚Ausdauer, Disziplin und Einsatzbereitschaft fortführen' – Rede von Bundesminister Otto Schily vor dem Deutschen Bundestag am 11. Oktober 2001. In: Bundesministerium des Innern (2004): Nach dem 11. September 2001. Maßnahmen gegen den Terror. Dokumentation aus dem Bundesministerium des Innern: 30-36. Online verfügbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2004/Nach_dem_11_September_2001_Massnahmen_Id_95066_de.pdf;jsessionid=E1F168A945AD97F71C21ED23EC68B039.2_cid156?__blob=publicationFile [12.08.2011]

Selbmann, Frank (2008): Verfassungsbeschwerde Julia Zeh, Frank Selbmann: § 4 Abs. 3 und § 4 Abs. 4 des Passgesetzes vom 19. April 1986 (BGBl. I S. 537) in der Fassung vom 20. Juli 2007 (BGBl. I 1566) verstoßen gegen Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 und Art. 12 Abs. 1 GG und sind nichtig. Online verfügbar unter: http://images.zeit.de/2008/06/ Verfassungsbeschwerde28012008.pdf [15.04.2015]

VDI/VDE Innovation + Technik GmbH (2009): Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen. Thema: Der Markt für Sicherheitstechnologien in Deutschland und Europa – Wachstumsperspektiven und Marktchancen für deutsche Unternehmen. Schlussbericht. Berlin. Online verfügbar unter: http://www.vdivde-it.de/publikationen/studien/marktpotenzial-von-sicherheitstechnologien-und-sicherheitsdienstleistungen. [23.07.2016]

Anhang

Anhang A: Interviewleitfaden für Fingerabdruckgeber

I. Anmeldung

Können Sie noch einmal an die Anmeldung zurückdenken, als Sie[71] (das Dokument beantragt/sich für das Verfahren registriert haben)? Wie ist das abgelaufen? Wie war das für Sie? (Ggfs. Nachfragen: Was waren Assoziationen, die Ihnen durch den Kopf gingen? Wie haben Sie die Anmeldung bzw. Registrierung erlebt? Was wurde erklärt? Welche Erklärungen hätten Sie sich gewünscht?)

Wenn Sie sich einmal zurückerinnern, was war der Grund, warum Sie sich (haben registrieren lassen/für bzw. dagegen entschieden, den Fingerabdruck aufzunehmen)? (Ggfs. Nachfragen: Was hat Sie überzeugt? Was sprach dagegen? Warum?)

Behörde: In welchem Zusammenhang haben Sie vorher schon von Biometrie gehört? Wie erklären Sie es sich, dass nunmehr ein Fingerabdruck in den Dokumenten gespeichert wird?

Was war das für ein Gefühl den Finger einscannen zu lassen? (Ggfs. Nachfragen: Hat es gleich funktioniert? Wenn nicht, warum? Wie war das? Wie war es, (k)ein Bild vom Fingerabdruck zu sehen?)

Wo werden die Daten eigentlich gespeichert?

II. Erfahrungen

Videothek/Supermarkt/Schule: Haben Sie nach der Registrierung schon mit dem FP bezahlt? Wenn ja, wie lief das ab? Wenn nein, wie meinen Sie, wird das ablaufen? (Ggfs. Nachfragen: Wie hat sich seither der Umgang mit dem Fingerabdruckscanner verändert?)

Schule: Welche Rolle spielt es für Dich, ob (andere) Kinder/Jugendliche per Fingerabdruckverfahren bezahlen?

Wie funktioniert der Umgang mit der Technik bei der Nutzung? Hat das (immer) gleich geklappt, dass der Scanner Sie erkennt? (Ggfs. Nachfragen: Wie war das Sie? Bzw. meinen Sie, dass der Scanner Sie immer gleich erkennt? Was meinen Sie, wie würden Sie

[71] Minderjährige Schüler wurden geduzt und Frageformulierungen altersgerecht angepasst.

damit umgehen, wenn das mal nicht klappt? Wie wäre das für Sie? Woran lag das/könnte das liegen? Wie gehen Sie damit um/werden damit umgehen?)

Wie würden Sie den Umgang mit der Technik beschreiben? (Ggfs. Nachfragen: Gibt es etwas Besonderes in der Benutzung des Verfahrens? Welche Rolle spielt Routine im Umgang mit dem Verfahren?)

Wie schätzen Sie es ein, dass mit dem Fingerabdruck 100-prozentig nur Sie identifiziert werden?

III. Bedeutungen

Hat sich mit der Registrierung das Bezahlen/Videoausleihen für Sie verändert? (*Schule*: Macht es einen [preislichen] Unterschied, wie man bezahlt?)

Ist das Verfahren ein Thema im Gespräch mit Bekannten/Freunden/Familie? (*Schule*: wer hat das seinerzeit entschieden? Wurde darüber diskutiert? Wenn ja, worüber wurde diskutiert?)

Welche Vorteile sehen Sie darin speziell den Fingerabdruckverfahren einzusetzen? (Ggfs. Nachfragen: Gibt es Unterschiede zu alternativen Verfahren? Können Sie sich vorstellen, warum gerade der Fingerabdruck eingesetzt wird?)

Welche Nachteile sehen Sie darin?

Wenn Sie an Ihren eigenen Fingerabdruck denken, was fällt Ihnen dazu spontan ein? (Ggfs. Nachfragen: Welche Bedeutung hat der Fingerabdruck? Welche Daten sind für sie generell persönlich wichtig? Welche Unterschiede würden Sie zwischen diesen machen?)

Welche Daten wurden eigentlich abgespeichert? Was meinen Sie, wo die Daten abgespeichert wurden? (Ggfs. Nachfragen: Haben Sie sich im Vorhinein damit beschäftigt, was mit dem Fingerabdruck und Ihren Daten passiert? Was könnte mit ihren Daten passieren?)

Können Sie sich vorstellen, dass jemand Interesse an Ihren Daten haben könnte? (Ggfs. Nachfrage: Wer? Warum?)

Es wird ja momentan viele über das Thema Datenschutz diskutiert. Welche Bedeutung hat Datenschutz für Sie? (Ggfs. Nachfragen: Was verstehen Sie darunter?)

Welche Vorteile/welche Nachteile sehen Sie in dem Verfahren?

IV. Kontexte

Das Fingerabdruckverfahren wird gegenwärtig immer häufiger eingesetzt. Aus welchen Bereichen kennen Sie das Verfahren?

Wie bewerten Sie das? (Wenn ja, nutzen Sie das auch selbst? Glauben Sie, das wird sich durchsetzen?)

Können Sie sich vorstellen, dass Sie den Fingerabdruck auch anderweitig einsetzen? Wo wäre es sinnvoll, wo nicht?

Wie würden Sie sich einschätzen: Sind Sie grundsätzlich jemand, der sich für Technik begeistern kann?

Mittlerweile ist das Abgeben von Fingerabdrücken im Reisepass obligatorisch, im Personalausweis außerdem freiwillig. Können Sie sich vorstellen, das zu nutzen?

Gibt es für Sie einen Unterschied zwischen der Nutzung des Fingerabdrucks hier (im Anwendungssetting) und dem durch das Amt? (wenn ja, worin liegt dieser?)

Gibt es vielleicht etwas, was wir bisher noch thematisiert haben, dass Ihnen in diesem Zusammenhang aber noch wichtig erscheint?

Haben Sie selbst noch Fragen zum Projekt?

Anhang B: Zusammenfassung

Die vorliegende Studie, die aus dem von der Deutschen Forschungsgemeinschaft geförderten Forschungsprojekt „Biometrie als ‚soft surveillance'. Zur Akzeptanz von Fingerabdrücken im Alltag" (Laufzeit Oktober 2010-Dezember 2013) heraus entstanden ist, untersucht die Akzeptanz von Fingerabdruckverfahren im Alltag in vier Anwendungsfeldern: als eine Bezahlmethode in einem Supermarkt und Schulen, als Modus der Zeiterfassung in einer Arztpraxis, als Zugangsmechanismus in einer Automatenvideothek sowie im Rahmen von behördlichen Anwendungen bei der ePass- und Personalausweisstellung. Sie befasst sich damit, warum Fragen nach der Akzeptanz von Fingerabdruckverfahren überhaupt erst aufkommen, wie Akzeptanz empirisch erfasst werden kann und interessiert sie sich insbesondere für die Verhandlung der der Bedeutung der Technologie im Rahmen von Sicherheits- und Überwachungsdiskursen. Vor diesem Hintergrund geben Interviews mit Nutzern und Beobachtungen von Registrierungs- und Nutzungssituationen Aufschluss darüber, dass sich Akzeptanz nicht schlicht in rationalen Abwägungen erschließen lässt, wie es die klassische Akzeptanzforschung vorschlägt. Die Arbeit untersucht, wie Akzeptanz gesellschaftlich hergestellt wird und dass sich hinter beobachtbarem Nutzungshandeln unterschiedliche Handlungsorientierungen verbergen, die ihre Bedingungen in einem spezifischen Wissen vom Fingerabdruck, situativen Deutungen und kontextuellen Regeln in den jeweils konkreten Settings der Anwendung des Fingerabdruckverfahrens finden.

The study bases on the project "Biometrics as 'Soft Surveillance'. On the acceptance of fingerprints" (funded by the German Research Foundation, 2010-2013) and aims to scrutinize the acceptance of fingerprint technologies in everyday life in the following contexts: a video rental store where it has been installed as a device for access procedures, a supermarket and school canteens where fingerprinting serves as an alternative payment device, a dental practice (time and attendance recording) and a national registration office where citizens apply for national identity schemes. It considers why acceptance of fingerprint technology becomes questionable, researches the role of discourses on security and surveillance and presents empirical findings on the conditions of acceptance, that have been gathered through qualitative interviews and participant observation. The results show that social acceptance is a heterogeneous phenomenon, not only because it depends on the situational features of dealing with the technology, but also on knowledge about the technologies and contextual rules in the specific areas of application.

Anhang C: Liste der aus der Dissertation hervorgegangenen Veröffentlichungen

2018

Zur Politik der Sicherheitsversprechen: die biometrische Verheißung *(zus. mit Christina Schlepper)*. In: Tobias Singelnstein/Jens Puschke (Hg.): Der Staat in der Sicherheitsgesellschaft. Schriftenreihe Staat – Souveränität – Nation. Beiträge zur aktuellen Staatsdiskussion. Wiesbaden: Springer VS: 79-99

2015

Gambling with the "Gift"? On the Relationship between Security Technologies, Trust and Distrust. The Case of Fingerprinting. In: Benjamin Rampp/Martin Endress (Hg.): Trust in Times of (In-)Security. On the Relationship between the Phenomena of Security and Trust. Behemoth. A Journal of Civilisation 8(1): 24-45. Online verfügbar unter: http://ojs.ub.uni-freiburg.de/behemoth/article/view/851/817

2014

Die gesellschaftliche Konstruktion von Sicherheit. Zur medialen Vermittlung und Wahrnehmung der Terrorismusbekämpfung *(zus. mit Susanne Krasmann/Reinhard Kreissl/Bettina Paul/Christina Schlepper)*. Schriftenreihe Forschungsforum Öffentliche Sicherheit, Berlin 2014. Online verfügbar unter: https://www.sicherheit-forschung.de/forschungsforum/schriftenreihe_neu/sr_v_v/SchriftenreiheSicherheit_13.pdf

'My fingerprint on Osama's cup.' On objectivity and the role of the fictive regarding the acceptance of a biometric technology *(zus. mit Susanne Krasmann)*. In: Surveillance & Society 12 (1): 1-14. Online verfügbar unter: library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Open_2014

2013

Big Data und Big Brother – was, wenn sie sich treffen? Über die vernachlässigte politische Dimension von Kontroll- und Überwachungstechnologien in der Akzeptanzforschung *(zus. mit Susanne Krasmann)*. In: Kriminologisches Journal 25(4): 242-259

Versicherheitlichung und Biometrie. Zur Verbreitung einer Kontrolltechnologie im Spannungsfeld von Staat, Ökonomie und Alltag *(zus. mit Jan Wehrheim)*. In: Daniela Klimke/Aldo Legnaro (Hg.): Politische Ökonomie und Sicherheit, Weinheim/Basel: Beltz Juventa: 303-318

Erklärung über professionelle Promotionsbetreuung

Hiermit erkläre ich, Sylvia Kühne, dass ich keine kommerzielle Promotionsberatung in Anspruch genommen habe. Die Arbeit wurde nicht schon einmal in einem früheren Promotionsverfahren angenommen oder als ungenügend beurteilt.

_____ _____

Ort/Datum Unterschrift Doktorand/in

Eidesstattliche Versicherung

Ich, *Sylvia Kühne*, versichere [1] an Eides statt, dass ich die Dissertation mit dem Titel:

„Sanfte Überwachung? Eine Untersuchung zur Akzeptanz von digitalen Fingerabdrucktechnologien im Alltag“

selbst und bei einer Zusammenarbeit mit anderen Wissenschaftlerinnen oder Wissenschaftlern gemäß den beigefügten Darlegungen nach § 6 Abs. 3 der Promotionsordnung der Fakultät Wirtschafts- und Sozialwissenschaften vom 24. August 2010 verfasst habe. [2] Andere als die angegebenen Hilfsmittel habe ich nicht benutzt. [3]

_____ _____

Ort/Datum Unterschrift