Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Ergebnisdokumentation

Workshop

‚Überwachung: Die Bedeutung technischer Innovationen und ihre gesellschaftlichen Auswirkungen‘

25./26. Februar 2015

Fraunhofer FOKUS

Protokolle: Nels Haake, Catharina Lüder, Julia-Sandrine Schröder
Zusammenfassung und Dokumentation: Gabriel Bartl
Organisation und Sekretariat: Helga Jäckel

Forschungsforum Öffentliche Sicherheit
Freie Universität Berlin, Carl-Heinrich-Becker-Weg 6-10, 12165 Berlin
Tel: +49 (0)30 838 58471, Fax: +49 (0)30 838 57399
gabriel.bartl@fu-berlin.de www.sicherheit-forschung.de

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Inhalt

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

1. Programm

Mittwoch, 25. Februar 2015

12:00 Uhr	Anmeldung und Begrüßungskaffee
12:30 Uhr	Begrüßung **Prof. Dr.-Ing.** Jochen **Schiller**, Freie Universität Berlin, Forschungsforum Öffentliche Sicherheit und Innovationszentrum Öffentliche Sicherheit
12:45 Uhr	Einführung und Vorstellung des Konzepts „Schaufenster Sicherheitsforschung“ **Dr.** Lars **Gerhold**, Forschungsforum Öffentliche Sicherheit **Dr.** Ulrich **Meissen**, Fraunhofer Fokus Vorstellung der Studie des Forschungsforums *„Überwachung: Die Bedeutung technischer Innovationen und ihrer gesellschaftlichen Auswirkungen“* **Dr. habil.** Nils **Zurawski** Kommentar zur Studie **Prof. Dr.** Klaus **Thoma**, Fraunhofer Ernst-Mach-Institut
13:45 Uhr	Kaffeepause
14:15 Uhr	*„Freiheit - Sicherheit - Überwachung - Recht“* **Prof. Dr.** Christoph **Gusy**, Universität Bielefeld *"Automatisierte Videoüberwachung als Sicherheitstechnologie? Einblicke in ihre massenmediale Repräsentation und die Perspektiven potenzieller Anwender"* **Dr.** Jens **Hälterlein**, TU Berlin *„Überwachungstechnologien im öffentlichen Raum“* Eric **Töpfer**, Deutsches Institut für Menschenrechte
15:30 Uhr	Kaffeepause
16:00 Uhr	Einführung **Dr.** Saskia **Steiger**, Forschungsforum Öffentliche Sicherheit *„Sensorbasierte Überwachung öffentlicher Räume am Beispiel eines Flughafens“* **Prof. Dr.-Ing.** Jochen **Schiller**, Freie Universität Berlin *„Neue Technologien – Zukunft der Videoauswertungssysteme“* **Dr.-Ing.** Markus **Müller**, Fraunhofer IOSB *„Überwachung und Datenschutz im öffentlichen Raum“* **Dr.** Rainer **Stentzel**, Bundesministerium des Innern
17:15 Uhr	Kaffeepause

17:45 Uhr Paneldiskussion: *„Überwachung: Die Bedeutung technischer Innovationen und ihrer gesellschaftlichen Auswirkungen aus Sicht politischer Entscheider“*

- Dr. habil. Nils Zurawski
- Dr. Ulrich Meissen, Fraunhofer Fokus
- Dr. André Hahn, MdB, Bundestagsfraktion DIE LINKE
- Nina Warken, MdB, Bundestagsfraktion CDU
- Gerold Reichenbach, MdB, Bundestagsfraktion SPD

Moderation: Konrad Litschko, taz.die tageszeitung

19:00 Uhr Abendessen

Donnerstag, 26. Februar 2015

08:30 Uhr Begrüßungskaffee

9:00 Uhr Überwachung: Die Bedeutung technischer Innovationen und ihre gesellschaftlichen Auswirkungen

Besuch Schaufenster Sicherheitsforschung (9:00 Uhr, 9:20 Uhr, 9:40 Uhr)
Stefan Pfennigschmidt (Fraunhofer Fokus)

AG I Soziale und ethische Implikationen von Überwachungstechnologien
Moderation: Dr. Benjamin Rampp (Universität Trier) und Gabriel Bartl (Freie Universität Berlin)

AG II Überwachung in der Praxis: Technische Innovationen und deren Potentiale
Moderation: Matthias Wählisch (Freie Universität Berlin) und Mark Palkow (daViKo - Gesellschaft für digitale audiovisuelle Kommunikation mbH)

AG III Politischer Wille und gesetzliche Grenzen im Umgang mit Überwachung
Moderation: Dr. Johannes Eichenhofer (Universität Bielefeld) und Nils Leopold (Büro Konstantin von Notz, MdB)

12:00 Uhr Präsentation und Diskussion der Arbeitsgruppenergebnisse

13:00 Uhr Gemeinsames Mittagessen

14:00 Uhr Ende der Veranstaltung

2. Fragestellung(en) und Zielsetzung(en) des Workshops

In öffentlichen wie wissenschaftlichen Debatten wird der Sinn und Zweck von Überwachung unterschiedlich bewertet. Auf der einen Seite wird Überwachungstechnologien eine wichtige Funktion bei der Verbesserung der Aufklärungsquote von Verbrechen attestiert und ihnen bei potenziellen Schadenslagen, Krisen oder Notfällen z. B. durch die frühzeitige Erkennung sich verdichtender Menschenmassen wichtige Präventionsfunktion zugeschrieben. Auf der anderen Seite wird ihr Potenzial hinsichtlich der Verhinderung von Straftaten oftmals angezweifelt und über Verdrängungseffekte, die von Überwachungskameras ausgehen, diskutiert. Dazu kommen Fragen zu Verhältnismäßigkeit und Diskriminierung, also beispielsweise ob der Eingriff in die Privatsphäre mit einem Gewinn an Sicherheit zu rechtfertigen ist. Eine umfassende Bewertung dieser verschiedenen Entwicklungen und Perspektiven setzt eine Differenzierung der Anwendungsfelder und Intentionen von Überwachung voraus. Dies will der Workshop „Überwachung: Die Bedeutung technischer Innovationen und ihrer gesellschaftlichen Auswirkungen“ gemeinsam mit Expertinnen und Experten aus Wissenschaft, Politik, Wirtschaft und Praxis leisten.

Ausgangspunkt des Workshops ist die Beobachtung, dass technische Innovationen nicht getrennt von ihren sozialen, ethischen und rechtlichen Implikationen gedacht werden können. Denn „Techniken sind nicht nur technische Installationen aus physischer Materie, Energie und Information, sondern zugleich auch material vermittelte soziale Institutionen“.[1] Am Beispiel von Überwachungstechnologien soll diese Beobachtung innerhalb des Workshops in der interdisziplinären Zusammenarbeit konkretisiert und fruchtbar gemacht werden.

Die analytische und praktische Trennung von technischen Innovationen und deren (oftmals nicht intendierten) Konsequenzen – z. B. in ingenieurwissenschaftlichen Kontexten der Technologieentwicklung – scheint, auch entgegen dem eigentlichen Anspruch der Sicherheitsforschung, noch immer gravierend auszufallen. Die vielfältigen Wirkungspotenziale von technischen Entwicklungen sollten aber nicht erst als zweiter Schritt im Sinne einer Technikfolgenabschätzung gedacht, sondern aktiv in den Entstehungsprozess integriert werden, so dass dieser Prozess von einem wechselseitigen interdisziplinären Austausch profitieren kann. Die Suche nach Möglichkeiten technologische Designprozesse partizipativer und transparenter zu gestalten ist in dieser Perspektive eine Voraussetzung für das Ziel der Abmilderung nicht intendierter sozialer, ethischer und rechtlicher Konsequenzen.

Insgesamt war der Workshop – hierbei insbesondere das *Schaufenster Sicherheitsforschung* – auch als Ergebnisplattform mehrerer BMBF-Projekte, die im Bereich der Überwachungsforschung angesiedelt waren, gedacht. Das *Schaufenster Sicherheitsforschung* versteht sich hierbei als Demonstrationsraum, in dem die komplexe Verzahnung von Technik und Gesellschaft und die sich daraus ergebenden Herausforderungen auf verschiedenen Ebenen plastisch gemacht werden kann.

[1] Rammert, Werner (2006). Technik, Handeln und Sozialstruktur: Eine Einführung in die Soziologie der Technik. Technical University Technology Studies, Working Papers, TUTS-WP-3-2006, S. 6.

3. Präsentation der Expertise

3.1 Technische Innovationen und deren gesellschaftliche Auswirkungen im Kontext von Überwachung

Dr. habil. Nils Zurawski (Universität Hamburg)

Die Studie ist zu finden unter www.schriftenreihe–sicherheit.de

Aufgabe der Expertise war es etwas über die Beziehung technischer Innovationen und ihrer gesellschaftlichen Auswirkungen auszusagen und zusammenzutragen. Ausgehend davon, dass Gesellschaft und Technik koevolutionär sind, also sich nur gegenseitig bedingend fort- und weiterentwickeln, untersucht diese Expertise die vielschichtigen Wechselwirkungen von Überwachungstechnologien und Gesellschaft. Technische Innovationen im Bereich der Sicherheit konzentrieren sich in der Hauptsache auf (digitale) Mess-, Regelungs-, oder Erfassungstechnologien, mit denen man „überwachen" kann. Grundlegend für die Betrachtungen ist die Annahme, dass es sich bei Technologien um eine materielle Kultur handelt, was bedeutet, dass Technologien Dinge darstellen, die symbolisch und ideologisch aufgeladen sind, Bedeutungen transportieren und somit politisch und sozial nie neutral sind. Technologien sind materialisierte Anwendungen von Wissen, mit denen umgegangen wird und welche Teil sozialer Beziehungen innerhalb von Gesellschaften darstellen.

Das gilt insbesondere für solche technischen Innovationen im Bereich von Sicherheit, die mit der Überwachung und Kontrolle von Menschen zu tun haben. Hierbei ist zunächst festzustellen, dass diese drei Begriffe – Sicherheit, Überwachung sowie Kontrolle – hinreichend unspezifisch sind und somit in der Regel ganz unterschiedlichen Interpretationen entsprechend verwendet werden. Mögliche Beurteilungen von Technologien und letztlich auch alle damit verbundenen Konsequenzen (und deren Einschätzungen) hängen von diesen Interpretationen ab. Keiner der Begriffe beschreibt ein Phänomen aus sich selbst heraus, weswegen es für die weitere Arbeit notwendig ist, hier eine Abgrenzung vorzunehmen und das Untersuchungsfeld zu definieren.

Untersuchungsfelder

Überwachung und Kontrolle sind sich ergänzende Ensembles von Handlungen, die zur Herstellung einer normativ konstruierten Sicherheit eingesetzt werden können. Grundlage dafür sind die darin eingeschriebenen Machtverhältnisse. Diese müssen nicht zwingend zwischen Staat und Bürgern bestehen, sondern können vielfältige, jeweils reziproke Konstellationen betreffen – Bürger-Bürger, Staat-Bürger, Unternehmen-Bürger. Die Macht kann dabei offen durch Zwang sicht- und spürbar werden oder verdeckt und subtil in so genannten Macht-Techniken wirken.

Die sozialen Beziehungen und Handlungsfelder zeichnen sich durch die Praktiken der Sammlung von Informationen und deren Kategorisierung sowie die Überprüfung von Personen aus, welche aufgrund asymmetrischer Herrschafts- und Machtverhältnisse möglich sind, manifestiert in der Verfügbarkeit entsprechender Technologien oder Verfahren zu Zwecken ihrer Lenkung, ihres Managements und ihrer Inklusion/Exklusion. Datenschutz stellt die Verregelung dieser Handlungen in Bezug auf dabei betroffene Informationsflüsse im Allgemeinen dar, in denen die Privatsphäre als zu schützendes Gut

eine zentrale Stellung einnimmt. Sicherheit als normierter Zustand und als Konstrukt gesellschaftlicher Aushandlungen dient als ein mögliches Argument für Überwachung und Kontrolle, während jene auch gänzlich ohne einen Verweis auf Sicherheit auskommen können.

Theoretischer Rahmen dieser Analyse ist eine auf Prävention hin orientierte so genannte Risikogesellschaft, in der die Antizipation von Risiken und deren beständige Abwehr zum Kern gesellschaftlicher Dynamik werden. Ob dabei Risiko und Gefahr verwechselt werden, wenn die Risiken so beständig und der Gesellschaft scheinbar so unvermittelbar sind, dass die Überwachung und Kontrolle sich auf alles und jeden auszudehnen droht, ist dabei eine der Kernfragen der vorliegenden Analyse.

Wird mit Sicherheit als einem zentralen Argument (z. B. „Videoüberwachung sorgt für Sicherheit im öffentlichen Raum“) jedoch die Implementierung einer technischen Innovation begründet, so kann sich aus dieser Verbindung eine vielfältige Dynamik entwickeln. Die daraus entstehenden Konsequenzen liegen jenseits der Technologie selbst. Auch darf Technik in diesen Fällen nicht als monokausal auf die Gesellschaft einwirkendes Phänomen verstanden werden. Vielmehr geht es darum, Prozesse zu analysieren, die sowohl die Bedeutungen von Technik in der Gesellschaft, damit verbundene mögliche Funktionswanderungen von Technik, die Argumentationslogiken, mit denen Technik umgeben wird sowie die Normen, die entweder entstehen oder die für die Zweckorientierung der Technologie selbst als gegeben vorausgesetzt werden, erfassen. Ob und wie Technik in einer Gesellschaft zielgerichtet – d.h. entsprechend eines mutmaßlichen Zweckes – eingesetzt werden kann, hängt auch davon ab, ob gesellschaftliche Konstellationen, Wünsche und Bedeutungszuschreibungen dies zulassen bzw. ermöglichen.

Beispiele technischer Innovationen

Diese sozio-technischen Wechselwirkungen werden an ausgesuchten Technologien exemplarisch nachvollzogen. Für diese Expertise wurden dafür vor allem solche Technologien betrachtet, die im Bereich Sicherheit technische Innovationen im weitesten Sinne darstellen und direkt oder indirekt zur Überwachung und Kontrolle von Raum, Bevölkerungsgruppen oder einzelner Personen eingesetzt werden können. Diese Beispiele sind im Einzelnen: Der Raum des Flughafens, als einem zentralen Ort von Sicherheit, sowohl im Bereich des Fliegens, als auch im Bereich des Passagiermanagements (was hier maßgeblich behandelt wird). Weiterhin werden die sozio-technischen Wechselwirkungen hinsichtlich Überwachung und Kontrolle im Bereich von Sicherheit im öffentlichen urbanen Raum betrachtet, insbesondere bezogen auf ein vernetztes Management der Stadt (smart city) sowie konkret am Beispiel von Stadionsicherheit, womit sich der Fokus auf einen abgegrenzten Raum richtet. Und schließlich wird im Kontext von Kriminalitätsbekämpfung die Technologie der BodyCams einer Betrachtung unterzogen und gezeigt wie sich hier die Wünsche an eine Technologie, die technischen Möglichkeiten und strukturellen Rahmenbedingungen (Datenschutz, Beschaffenheit des Raumes, Möglichkeiten der Prävention) gegenseitig bedingen, aber eben auch widersprechen.

Anhand dieser Beispiele werden die möglichen Implikationen technischer Anwendungen im Kontext von Sicherheit und Überwachung im Hinblick auf gesellschaftliche Dynamik erörtert. Diese Beispiele stellen Anschauungsmodelle dar, bei denen es weniger um kausale Begründungs- oder Beweisketten geht, sondern vielmehr darum, die durch die Einführung oder den Einsatz bestimmter Technologien berührten sozialen Dimensionen zu erörtern und weitere Fragen zu formulieren. Der Nutzen von

idealtypischen Handlungsmodellen oder vermeintlichen Kausalketten ist wenig hilfreich, wenn es darum geht die möglichen Tragweiten von Technologien zu analysieren. So können z. B. Kameras je nach Wunsch wahlweise Kriminalität reduzieren, Terror bekämpfen, Verhalten normieren oder eine Bedrohung für die Privatsphäre darstellen. Letztlich kann eine Kamera aber nur Bilder aufnehmen und somit nur als Träger von Bedeutungen, eingebettet in soziale und räumliche Kontexte, die Ziele erreichen, die der Technik selbst zugeschrieben werden. Ziele werden hier mit den tatsächlichen Funktionsweisen verwechselt. Analog gilt das auch für andere Technologien in anderen Anwendungsfeldern. Die entsprechenden Analysen und Fragen bezogen auf die eben genannten Felder werden in der Expertise exemplarisch durchgespielt und mit aufgezeigt.

Handlungsempfehlungen für die Sicherheitsforschung im Kontext von Überwachung

In der Sicherheitsforschung gibt es unterschiedliche Akteursgruppen – Politik, Wissenschaft sowie zivil-gesellschaftlich Akteure und Unternehmen. Diese Gruppen lassen sich an ihrer internen Logik wie folgt unterscheiden:

- *Politik*: Ausübung von Macht, Gestaltung der Politik und grundlegend verantwortlich für die zivile und militärische Sicherheit.
- *Wissenschaft*: Erkenntnisinteresse, Generierung von Wissen, Berater der Politik, Finanzierung der eigenen Forschung
- *Unternehmen / zivile und staatliche Akteure*: Profit (monetär und symbolisch), praktischer Nutzen von Innovationen

Den Empfehlungen, die sich an die genannten Akteursgruppen richten, sind drei übergeordnete Prinzipien vorangestellt: Kommunikation, Reflexion und Transparenz. Kommunikation bedeutet sowohl einen Dialog mit der Öffentlichkeit, als auch eine Kommunikation über Ziele, Strategien und Vorstellungen zwischen den Partnern beliebiger Sicherheitsforschungsprojekte. Reflexion meint das Nachdenken über das eigene Handeln und fragt nach der gesellschaftlichen Verantwortung. Verantwortung kann nur übernommen werden – und im Gegenzug als Merkmal für Güte beansprucht werden – wenn Klarheit über das eigene Tun und die dahinter stehenden Motivationen und Verbindungen nach außen herrscht. Daher ist Transparenz das dritte Grundprinzip.

Politik

- Sicherheit muss als gesellschaftliche Aufgabe begriffen werden. Dabei sollte eine Perspektive gewählt werden, die Sicherheit als etwas für jemanden und nicht gegen jemanden betrachtet. Folglich muss auch eine Reflexion über den verwendeten politisch-strategischen Sicherheits-begriff erfolgen.
- Der Einsatz von Technologie als Instrument der zivilen Sicherheit setzt Evaluationsprozesse voraus. Was oder für wen bringt Überwachung etwas? Was sind die gesellschaftlichen Kosten?
- Kommunikation über die Zusammenhänge von Technologie und Sicherheit muss transparent sein: Was ist unsicher? Wer oder was ist das Risiko? Wer ist das Ziel von Überwachung?

- Es sollten alternative Lösungsansätze zum Umgang mit Unsicherheit vorgezogen werden, die nicht primär auf einer Technologie basieren, sondern gesellschaftlich orientiert sind.
- Vermeidung alarmistischer Politik, die mit der Angst vor Gefahren operiert und vermeintlich alternativlose Maßnahmen vorschlägt.
- Personelle und institutionelle Verquickungen müssen transparent gemacht werden, um Vertrauen zu schaffen und Verantwortlichkeiten offen zu legen und diese einfordern zu können. Sicherheitsforschung ist keine Industriepolitik.

Wissenschaft

- Wissenschaft muss aktiv auf die Gestaltung einer anderen Sicherheitsforschung einwirken. Es geht um mehr als nur Machbarkeit (Ingenieurwissenschaften) oder Akzeptanzforschung (Sozialwissenschaften), nämlich darum kritisch und konstruktiv an neuen inklusiven Gesellschaftsmodellen zu arbeiten, in denen Sicherheitstechnik nicht primär Technologien der Abwehr und Überwachung sind.
- Wissenschaft muss Verantwortung für ihre Konzepte oder Produkte übernehmen, d.h. auch über den Sinn und weiteren Zweck von Technik zu reflektieren und Grenzen der Forschung definieren.
- Mögliche personelle Verquickungen mit Industrie, Forschungsförderern oder der Politik sollten transparent gemacht werden.
- Sicherheit als Konzept muss beständig reflektiert werden. Dies kann durch den Austausch zwischen den Disziplinen gestärkt werden

Unternehmen / zivile und staatliche Akteure

- Interessen und Motivationen, z. B. bei personellen und institutionellen Verbindungen zu Politik oder Wissenschaft sollten transparent gemacht werden.
- Die Kommunikation muss mit den anderen Akteursgruppen über konkrete Maßnahmen hinweg erfolgen. Das bedeutet auch die Reflexion über den Begriff der Sicherheit.

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

3.2 Kommentar zur Expertise

Prof. Dr. Klaus Thoma (Fraunhofer Ernst-Mach-Institut)

Die Idee des Workshops mit zwei konträren Positionen – die sozialwissenschaftliche Perspektive der Expertise wird von einem Technikwissenschaftler kommentiert – ein diskursives Feld für nachfolgende Diskussionen bereitzustellen erwies sich als guter Einstieg in die Thematik. Klaus Thoma als technikwissenschaftlicher Fürsprecher und Repräsentant kommentierte dann auch einige Stellen der Expertise kritisch, mit denen er nicht übereinstimmte.

So machte Thoma darauf aufmerksam, dass innerhalb der Expertise Sicherheit als normierter Zustand bezeichnet wurde, der Überwachung und Kontrolle gewissermaßen legitimiere. Dies wurde negiert, da Ingenieure die Produktion von Sicherheit nicht zwangsläufig mit Überwachung gleichsetzen würden und sich in ihrem Selbstverständnis vielmehr der Sicherheit verschreiben als den radikalen Ausbau von Überwachung gutzuheißen.

Innerhalb der Expertise wurde zudem angezweifelt, ob soziale und politische Probleme idealerweise mittels technischer Mittel gelöst werden sollten, was Thoma zwar genauso sah, an welchem Punkt er aber darauf hinwies, dass Technologien sehr wohl zur Verbesserung von Problemlagen dieser Art dienlich sein können. In diesem Zusammenhang referierte er über das Beispiel zu Videoüberwachung in Mexico City. Hier orientierten sich die Menschen zu ihrer eigenen Sicherheit an der überwachenden Infrastruktur. Als diese wieder abgebaut werden sollte, kam es sogar zu Protesten dagegen. An diesem Beispiel lasse sich also die Bedeutung und das Potenzial von Technologien für gesellschaftliche Prozesse erkennen, so dass auch die Behauptung in der Expertise, dass die Wirkung von Technik zumeist überschätzt werde nicht gestützt werden könne.

Wichtigster Kritikpunkt war allerdings die Szenarien-Kritik innerhalb der Expertise. Szenarien seien nämlich keinesfalls als ‚schlechteste Variante' des Umgangs mit Unsicherheit zu bezeichnen; vielmehr würden sie erwiesenermaßen zur Abmilderung von Naturkatastrophen beitragen wie es ein eigenes Projekt mit der US-amerikanischen Stadt Boston, die regelmäßig mit den Folgen des Klimawandels (z. B. in Form von Überschwemmungen) zu kämpfen hat, belegt. Diese Auswirkungen sind real, so dass auch der Gedanke, dass Risiken von der Industrie erfunden werden, um Lösungen in Produktform zu generieren, abwegig sei. Auch die Befürchtung, dass Szenarien ein Eigenleben entfalten, das in einem ständigen Ausnahmezustand mündet, bezeichnete Thoma als schwer nachvollziehbar.

Über die Forderungen innerhalb der Handlungsempfehlungen der Expertise herrschte dagegen größtenteils Einigkeit. So erfülle die technikwissenschaftliche Forschung bereits die angebrachten Gütekriterien wie Kommunikation, Reflexion oder Transparenz. Am Beispiel des BMBF-Sicherheitsforschungsprogramms, in dem alle Projekte und deren Ergebnisse einsehbar sind, manifestiere sich diese Empfehlung bereits in beispielhafter Manier.

Schließlich richtete Thoma noch das Wort an die sozialwissenschaftliche Community mit dem Wunsch, dass diese auch einmal stärker voran gehen solle – nach dem Motto: „Wir haben jenes soziale Problem – habt ihr nicht eine technische Lösung dafür?". Insgesamt wurde der Kommentar somit seiner

Positionierung innerhalb des Workshops als technikwissenschaftliche Anreicherung zu einer rein sozialwissenschaftlichen Perspektive gerecht.

4. Kurzfassungen der Fachvorträge

Die Folien zu den Vorträgen sind verfügbar unter www.sicherheit-forschung.de/workshops

4.1 Freiheit – Sicherheit – Überwachung – Recht

Prof. Dr. Christoph Gusy, Universität Bielefeld

Die rechtliche Perspektive auf Überwachung – der Fokus des Vortrags lag auf Videoüberwachung – bewegt sich im Spannungsfeld zwischen Freiheit und Sicherheit. Freiheitsrechte und Freiheitseinschränkungen stehen somit in einem potenziell konfliktären Verhältnis zu als notwendig erachteten Strategien der Gefahrenabwehr.

Die Videoüberwachung als spezielle Form der Überwachung ist in öffentlichen Räumen in Deutschland dabei generell nur als offene Form zulässig. Dagegen ist heimlich durchgeführte Videoüberwachung nur möglich, wenn besondere Gefahrenlagen vorliegen oder im Falle der Überwachung besonders verdächtiger, gefährlicher oder gefährdeter Personen (§§ 100h StrPrO, § 25 ASOG). Wer sich also in die Öffentlichkeit begibt, kann keinen Schutz vor Beobachtung in Anspruch nehmen, wohl aber das Recht auf Anonymität. Des Weiteren ist der Schutz vor Aufnahme, Aufzeichnung und Verarbeitung von Informationen daran gebunden wie die Ausweichmöglichkeiten bei der Nutzung von Öffentlichkeit ausgestaltet sind. Die Erhebung, Speicherung und Verarbeitung personenbezogener Daten muss somit gewisse Anforderungen erfüllen, die sich nach drei Kriterien bestimmen lassen. Erstens ist entscheidend wer die Datenerhebung und -verarbeitung vornimmt („öffentliche“ oder private Stellen). Zweitens ist zu klären, welche Orte betroffen sind („öffentlich zugängliche Orte“ oder solche, die nur bestimmten berechtigten Personen vorbehalten sind). Drittens ist nach dem Zweck zu fragen. Hierfür gelten dann unterschiedliche Sondergesetze, welche den Grundrechtsschutz partiell ausweiten und partiell einschränken. Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist zudem nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Grundsätzlich lassen sich drei denkbare Freiheitseinschränkungen durch öffentliche Videoüberwachung identifizieren. Vermeidungseffekte, Einschüchterungseffekte und Zweckentfremdung der erhobenen Daten. Vermeidungseffekte bezeichnen hierbei Verdrängungseffekte in einer Weise, dass potenziell Betroffene die Nutzung der überwachten Einrichtungen, Anlagen u.a. vermeiden, indem sie auf die Leistungen verzichten oder andere, nicht überwachte Einrichtungen nutzen. Einschüchterungseffekte bewirken, dass sich potenziell Betroffene unfrei verhalten; und zwar umso mehr, je weniger sie den konkreten Überwachungszweck kennen oder vom Missbrauch der Überwachung ausgehen. Eine Zweckentfremdung bestimmt sich durch die Informationsverwendung zu anderen als den Überwachungszwecken. Sind Daten also einmal erhoben, gespeichert und ggf. personalisiert, so können

Betroffene deren Verwendung nicht mehr kontrollieren. Letztere greifen in die informationelle Selbstbestimmung, erstere hingegen (auch) in andere Handlungsfreiheiten oder Nutzungsrechte ein.

Die genannten freiheitseinschränkenden Aspekte hängen allerdings nicht notwendig davon ab, dass die Überwachung tatsächlich stattfindet oder funktioniert. Sie kann auch allein von drei Faktoren abhängen: der bloßen Ankündigung, der erkennbaren Installation der Vorkehrungen, auch wenn diese abgeschaltet oder funktionsuntüchtig sein können, von stattfindender Überwachung, auch wenn diese keine personenbezogenen Informationen herstellt, wenn Betroffene mit Personenbezug rechnen oder ihn nicht ausschließen können. Berücksichtigungsfähige Ursachen von Freiheitseinschränkungen können also die Öffentlichkeit der Maßnahme selbst sein sowie ihr Stattfinden oder Erwartungen Betroffener (fehlende Kontrollmöglichkeiten oder fehlendes Vertrauen). Verdrängungseffekte hängen dagegen wesentlich ab von der (rechtlichen oder faktischen) Angewiesenheit auf diesen Raum, vom Vorhandensein (oder Fehlen) möglicher Alternativen und von der Nutzungssituation (informiert oder nicht-informiert; spontan oder überlegt; entscheidungs-/abwägungsfähig oder nicht). Einschüchterungseffekte hängen schließlich nach der Rechtsprechung wesentlich ab vom (möglichen) Wissen um das Stattfinden von Überwachung, wenn Betroffene keinen Anlass zu der Maßnahme gegeben haben, vom (möglichen) Wissen um das Stattfinden bei gleichzeitigen Nichtwissen um Zweck oder Ausgestaltung der Überwachung (personenbezogen oder nicht; mit oder ohne Aufzeichnung usw.), von dem (möglichen) Wissen über Streubreite, Nebenwirkungen, Verwendung bzw. Missbrauchbarkeit der Überwachung sowie von der „Massivität der Observation bzw. Registrierung“.

Ein begründeter Zweck von Videoüberwachung kann einerseits in der Abwehr näher bestimmbarer Gefahren, die Betroffenen drohen können (etwa aus der Funktion, der technischen Ausgestaltung, möglichen Störungen oder Kapazitätsgrenzen einer Einrichtung), liegen. Andererseits ist die Abwehr bestimmbarer Gefahren, die von Nutzern ausgehen können (etwa durch Nutzung von Gelegenheiten zur Straftaten in Menschenmengen) hier relevant. Die Zweckentfremdung tritt hierbei oftmals als juristisches Problem in Erscheinung, da es immer häufiger zu einer Verschiebung des Zwecks in Richtung Strafverfolgung kommt.

Die Rechtsprechung im Kontext von Videoüberwachung zur Gefahrenabwehr erfordert insgesamt die Berücksichtigung der folgenden Aspekte:

- Eine nachvollziehbare und nachvollziehbar dokumentierte Gefahranalyse (auch für „Kriminalitätsschwerpunkte“, „gefährliche“ oder „gefährdete“ Orte)
- Eine Abgrenzung der beobachteten Orte
- Eine hinreichend konkrete Zweckbestimmung der Überwachung (nicht bloß: generelle Senkung der Kriminalität an einem Ort)
- Nachweis der Notwendigkeit eines Personenbezuges der Überwachung und der Notwendigkeit der Aufzeichnung von Aufnahmen
- Eine Wirkungsprognose (können die konkreten Gefahren vor Ort durch eine Videoüberwachung überhaupt abgewehrt werden?), wobei bloße Verdrängungseffekte nicht stets zur Unzulässigkeit führen sollen

- Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit der Überwachungsmaßnahmen
- Eine rechtzeitig erkennbare und eindeutige Ankündigung der Maßnahme

In diesem Zusammenhang sind die derzeit verschiedenen Diskussionen zu betrachten. So wird versucht Fragen der Standardisierung und Zertifizierung typischer Gefahranalysen und Wirkungsprognosen zu klären und über Zertifizierungspflichten für Überwachungstechniken nachgedacht. Die Notwendigkeit begleitender periodischer Überprüfungen der weiteren Zulässigkeit bzw. Erforderlichkeit von Überwachungsmaßnahmen wird außerdem reflektiert.

4.2 Automatisierte Videoüberwachung als Sicherheitstechnologie? Einblicke in ihre massenmediale Repräsentation und die Perspektiven potenzieller Anwender

Dr. Jens Hälterlein, Technische Universität Berlin

Der Vortrag basierte auf den Ergebnissen des BMBF-Projektes MuViT, insbesondere des an der Universität Potsdam angesiedelten Forschungsteiles. Überwachung wurde hierbei auf zwei Ebenen aufgegriffen und analysiert: Erstens wurde mittels der Methode der wissenssoziologischen Diskursanalyse (WDA) der öffentliche Diskurs zu Überwachung und Überwachungstechnologien analysiert. Zweitens wurde innerhalb von qualitativen Interviews die Perspektive von Anwendern von Überwachungstechnologien – in diesem Fall der Polizei – berücksichtigt. Grundsätzlich ging es also um die Frage wie verschiedene Akteure um eine legitime Interpretation von automatisierter Videoüberwachung ringen. Als theoretische Hintergrundfolie der Darstellung dienten die einschlägigen sozialwissenschaftlichen Erkenntnisse zum Thema Überwachung. Im Falle von automatisierter Videoüberwachung konnte somit festgehalten werden, dass die Interpretationsleistungen zunehmend vom Menschen zu technischen Systemen verschieben, was zwar nicht bedeutet, dass Technik neutral ist – denn Algorithmen werden ja auf Basis normativer Grundannahmen programmiert – aber zu einer neuen Qualität von Überwachung führt. In diesem Zusammenhang wäre auch zu hinterfragen inwieweit Risikokalkulationen als Formen sozialer Kontrolle zu betrachten sind und in welcher Relation überhaupt Überwachung und soziale Kontrolle zueinander stehen, denn diese beiden Phänomene müssen nicht zwingend deckungsgleich sein. Die neue Qualität von automatisierten Formen der Überwachung manifestiert sich schließlich in der Fokussierung auf bestimmte kritische Situationen, wobei sich das Interesse weg vom Individuum in Richtung der Detektion von bestimmten Situationen bewegt. Diese Veränderung spiegelt sich etwa in neuartigen Strategien bei der Konzeption von öffentlichem Raum wider, der so gestaltet werden soll, dass Kriminalität durch die Anordnung und Ausgestaltung von räumlichen Strukturen erschwert wird. Videoüberwachung und automatisierte Mustererkennung lassen sich in diesem Sinne als soziale Konstruktionen operationalisieren, da in deren Funktions- und Arbeitsweisen immer sozial konstruierte Verständnisse von Normalität und Devianz eingeschrieben sind.

Die empirischen Analysen zum öffentlichen Diskurs führten im Ergebnis einer Medienanalyse zur Identifikation von vier Diskursen mit denen automatisierte Videoüberwachung als legitime bzw. illegitime Technologie konstruiert wurde. Von diesen vier Diskursen wurden drei näher vorgestellt: ein

Sicherheitsdiskurs, ein Effizienzdiskurs und ein Datenschutzdiskurs. Im Sicherheitsdiskurs werden die Konsequenzen von Kriminalität thematisiert, die sich durch automatisierte Überwachungstechnologien verhindern bzw. eindämmen lassen, was letztere legitimieren soll. Der Effizienzdiskurs beschreibt die vermeintlich höhere Effizienz von technischen Systemen der Kriminalitätserkennung und -bekämpfung, während der Datenschutzdiskurs das Mittel der Videoüberwachung mit möglichen Verletzungen des Rechts auf informationelle Selbstbestimmung in Verbindung bringt.

Im öffentlichen Diskurs wurden aber auch bestimmte Thematiken nicht berücksichtigt. So konnten innerhalb der Diskursanalyse nicht die Ursachen von Kriminalität identifiziert werden. Außerdem standen auch Phänomene, die sich aus automatisierter Mustererkennung ergeben nicht im Fokus der medialen Aufbereitung. Das Diskriminierungspotenzial (z. B. aufgrund von Alter, Ethnizität oder Geschlecht) von solchen Technologien als Ausdruck sozialer Ungleichheiten wurde demgemäß nicht thematisiert, genauso wie die Dequalifizierung der ohnehin schon im Niedriglohnsektor angesiedelten Sicherheitsarbeit. Die Kritik automatisierter Videoüberwachung beschränkt sich somit vor allem auf die Anmahnungen von Freiheitseinschränkungen und Eingriffe in Persönlichkeitsrechte. Die Frage nach den sozialen Ursachen von Kriminalität wird also fast vollständig aus dem Diskurs exkludiert, ebenso wie an eine solche Problemdefinition anschließende sozial- und arbeitsmarktintegrative Maßnahmen. Die Legitimität automatisierter Videoüberwachung wird damit als eine bloße Frage technischen Scheiterns einerseits und des Versagens bürokratischer Kontrolle andererseits inszeniert. Soziale Risiken im eigentlichen Sinne spielen keine Rolle. Man könnte also sagen, dass Überwachung als eine Praxis konstruiert wird, die einen rein technischen Prozess darstellt, der weder soziale Voraussetzungen noch soziale Folgen hat.

Auf Seiten der Anwender wurden Polizeibeamte interviewt, die bei LKAs und der Bundespolizei Sicherheitstechnologien bzw. deren Einsatz bei Großveranstaltungen verantworten. Bei den Polizisten ließen sich zum Teil deutlich abweichende Positionen identifizieren, die zwischen Prävention (Bundespolizei) und Repression (LKA) als Zweck und Nutzen von Videoüberwachung oszillierten. Bei allen interviewten Beamten konnte aber eine abweichende Position gegenüber dem Automatisierungsgrad der Technologie identifiziert werden, der im Effizienzdiskurs als sinnvoll erachtet wurde. Dem Versuch eines einfachen Ersetzens von menschlichen Kognitionen und Erfahrungswerten durch automatisierte Systeme standen die Interviewten kritisch gegenüber. Aus der Polizeiperspektive ließ sich Videoüberwachung folglich als Hilfsmittel, aber nicht als Allheilmittel bewerten. Die Nutzung von Überwachungstechnologien wurde vielmehr als Einzelkomponente in einem komplexen Zusammenspiel verschiedener Akteure betrachtet.

4.3 Überwachungstechnologien im öffentlichen Raum

Eric Töpfer, Deutsches Institut für Menschenrechte

Ausgangspunkt der Beschäftigung mit Überwachungstechnologien im öffentlichen Raum war der Begriff der Innovation: „Als Innovation werden materielle und symbolische Artefakte bezeichnet, welche Beobachterinnen und Beobachter als neuartig wahrnehmen und als Verbesserung gegenüber dem Bestehenden erleben“ (Braun-Thürmann 2005, S. 6). An dieser Definition lässt sich die Bedeutung der individuellen Komponente des Wahrnehmens und Erlebens von bestimmten Artefakten ablesen. In diesem Sinne geht es bei der Bewertung von Technologien nicht allein um die Analyse von gesellschaftlichen Auswirkungen in einem monokausalen Zusammenhang von Ursache und Wirkung (Technische Innovationen wirken auf die Gesellschaft), sondern genauso in umgekehrter Weise um soziale Konstruktionsleistungen, welche zu Bedeutungszuschreibungen und Nutzungsvisionen von Technologien führen.

Die Entstehung von Innovationen wurde nach der Konzeptualisierung von Weyer (1997) in drei Phasen unterteilt: Entstehung, Stabilisierung und Durchsetzung. Diese Phasen werden jeweils von unterschiedlichen sozialen Netzwerken getragen. Diese Netzwerke bestehen immer aus einer Vielzahl von Akteuren mit unterschiedlichen Interessen, weshalb sich Überwachungstechnologie auch als ‚Thing‘ begreifen lässt. Dieser Verweis stammt von Latour, der darauf aufmerksam machen möchte, dass der Begriff des ‚Thing‘ auf Versammlungen verweist, die den Sinn hatten Aushandlungsprozesse über bestimmte Themen voranzutreiben und als nordische Wiege der Demokratie bezeichnet werden. Übertragen auf Überwachung bedeutet dies, dass sowohl die Technikgestaltung als auch deren Nutzung immer aus divergierenden Interessenlagen resultieren.

Am Beispiel der Videoüberwachung in den Zügen der Berliner Verkehrsbetriebe (BVG) lässt sich eine solche Nutzungsverschiebung – von *safety*- zu *security*-Aspekten – aufgrund von Interessenverlagerungen beobachten. Ursprünglich sollten die Kameras lediglich detektieren, ob der Bahnsteig frei ist und die Spiegel an den Bahnsteigen ersetzen, bis dann das Interesse am aufgezeichneten Videomaterial im Zusammenhang mit Straftaten in den BVG-Waggons geäußert wurde.

Das Beispiel zeigt, dass Technik nicht unbedingt als eigenständiger Akteur betrachtet werden muss (wie innerhalb der Akteur-Netzwerk-Theorie), aber technische Artefakte durchaus politisch interpretiert und somit auf sozialer Ebene relevant werden können. In dieser Sichtweise generiert Technik strukturelle Veränderungen, die wiederum soziales Handeln potenziell beeinflussen und damit Pfadabhängigkeiten generieren.

Solche Pfadabhängigkeiten lassen sich etwa am Beispiel von Crime Mapping Software nachvollziehen. Hier schafft die Wahl des Algorithmus Pfadabhängigkeiten, indem bestimmte Gebiete nach der Logik des Algorithmus zu Risikogebieten deklariert werden, in denen die Polizei Sondervollmachten genießt. Technische Artefakte schaffen auf diese Weise soziale Realitäten. Ein anderes Beispiel wäre die schlechte Trefferquote von DNA-Analysekitts, die dazu führte, dass Großbritannien davon keinen Gebrauch machte; im Gegensatz zu Deutschland.

Dass der soziale Kontext für die Nutzung von Überwachungstechnologien eine zentrale Rolle spielt, machte ein historischer Abriss zur Entwicklung von Videoüberwachung deutlich. Der Terminus ‚CCTV‘

verweist zunächst darauf, dass die ursprüngliche Intention nicht auf Überwachung, sondern auf dem Fernsehen lag. Aus dieser Funktion wurden schließlich unterschiedlichste Nutzungsvisionen entwickelt, deren Durchsetzung oftmals vom sozialen Kontext abhing. So wurde die Möglichkeit eines Drohnenkrieges bereits im Jahr 1927 diskursiv erörtert, auch wenn die Übersetzung in technische Artefakte ausblieb. Die ersten Nutzer von Videoüberwachung waren dann die amerikanischen Elektrizitätswerke, wie es u.a. ein Spiegel-Artikel aus dem Jahr 1953 belegt. Interessant war, dass in diesem Artikel auch schon die Big Brother-Debatte geführt wurde. Ausgehend von der Überwachung von Elektrizitätswerken ist CCTV dann jedenfalls weiter diffundiert. In den 60er/70er Jahren wird Videoüberwachung dann mit der Bekämpfung von Straßenkriminalität in Großbritannien und den USA in Verbindung gebracht. Zu diesem Zeitpunkt folgt die Zuschreibung noch der Logik der Strafverfolgung, was auch ein Grund für die anhaltende Weiterverbreitung von CCTV war, denn aufgrund der nicht gegebenen Effektivität wurde CCTV zu diesem Zweck wieder eingestellt. Für die 80er Jahre lässt sich im Kontext von Überwachung die Volkszählung in Deutschland nennen, die aufgrund von massiven Protesten erst im Jahr 1987 durchgeführt werden konnte. Im damit zusammenhängenden Volkszählungsurteil wurde zum einen das Recht auf informationelle Selbstbestimmung verankert. Zum anderen wurden CCTV-Anlagen in Deutschland im Zuge der Proteste wieder abgebaut. Allerdings wurde die Videoüberwachung von Demonstrationen auf rechtlicher Ebene dennoch bald danach eingeführt, indem die Versammlungsgesetze dahingehend angepasst wurden. Erst in den 90er Jahren lassen sich öffentliche Debatten um polizeiliche Videoüberwachung öffentlicher Straßen und Plätze identifizieren, was Rückschlüsse auf eine Veränderung sozialer Kontextfaktoren zulässt. Interessant ist in diesem Zusammenhang schließlich ein Pilotprojekt zu Videoüberwachung, das 1996 in Leipzig durchgeführt wurde. Dieses Projekt wurde von politischer und behördlicher Seite als erfolgreich tituliert. So behauptete etwa der Bund Deutscher Kriminalbeamter Videoüberwachung hätte das Potenzial, Kriminalität um 80 Prozent zu reduzieren. Insgesamt lässt sich für den deutschen Fall dennoch nur ein begrenzter Grad an Normalisierung von CCTV verzeichnen, wenn man Deutschland etwa mit Großbritannien oder den Niederlanden vergleicht, da hierzulande die polizeiliche Verwendung von Videoüberwachung lediglich auf 60 bis 70 Städte zutrifft. Dennoch macht der historischer Abriss deutlich, dass das Verhältnis von Technik und Gesellschaft nicht monokausal zu verstehen ist, sondern als gegenseitiges Beeinflussungsverhältnis. In dieser Sichtweise lassen sich technische Innovationen dann auch erst als solche erkennen und nutzen, wenn der soziale Kontext ihre Diffusion in die eine oder andere Richtung interpretierbar macht.

Die Bewertung technischer Innovation ist schließlich eine Herausforderung für das sogenannte *Technology Assessment*. Hierbei geht es erstens um die Kontrolle des Erfolgs von neuen Techniken. Allerdings lässt sich Erfolg auch immer als *success by failure* interpretieren, wenn darauf verwiesen wird, dass Funktionsweisen optimiert werden können und sich dadurch ein Erfolg absehen lässt. Prinzipiell ist der Erfolg von technischen Innovationen auch schwer zu messen und zu quantifizieren. Eine zweite Alternative, welche die Methode des Technology Assessment bereitstellt, spiegelt sich in einer Art Wirkungsforschung wider. Doch auch die Wirkung ist ein abstraktes Konstrukt und es besteht hierbei die Gefahr von Verallgemeinerungen, wenn der spezifische Einsatz- und Nutzungskontext nicht mitberücksichtigt wird. Eine dritte Bewertungsoption bietet das *Constructive Technology Assessment*, welches die interdisziplinäre Zusammenarbeit bereits im Entwicklungsprozess bezeichnet. Im Rahmen

des *Constructive Technology Assessment* bieten sich drei Möglichkeitsfenster zur Einflussnahme. Erstens die Prüfung der innovativen Idee auf Sinnhaftigkeit im Anwendungskontext durch alle beteiligten Stakeholder. Zweitens kann die Entwicklung von Prototypen zur Evaluation an einem konkreten Beispiel verwendet werden. Drittens führt die Frage der Marktkonstitution wiederum zum Anwender, wenn etwa Fragen der Akzeptanz im Entwicklungsprozess Beachtung finden. An diesem Punkt lassen sich allerdings Zielkonflikte vermuten, wenn die Frage beantwortet werden muss, ob es um Sicherheits- oder Hightech-Forschung geht; ob also der Zukunftsmarkt der Sicherheitstechnologien bedient werden soll oder die Sicherheit und das subjektive Sicherheitsgefühl der Menschen.

4.4 Sensorbasierte Überwachung öffentlicher Räume am Beispiel eines Flughafens

Prof. Dr.-Ing. Jochen Schiller, Freie Universität Berlin

Das interdisziplinär angelegte BMBF-Forschungsprojekt SAFEST (Social-Area Framework for Early Security Triggers at Airports) wurde als Versuch präsentiert, sensorbasierte Überwachung in der Kritischen Infrastruktur des Flughafens zu etablieren und dabei soziale, ethische und rechtliche Grundsätze maximal zu berücksichtigen. Konkreter Ausgangspunkt der SAFEST-Technologie ist die Reduzierung von Risiken im öffentlichen Raum auf der einen Seite bei gleichzeitiger Aufrechterhaltung des Schutzes der Privatsphäre auf der anderen Seite. Der Fokus von SAFEST liegt dabei auf der Verhinderung von Massenpaniken und einer Arealüberwachung des Flughafengeländes, um unerlaubtes Eindringen zu verhindern. Das Projekt trägt auf diese Weise der Beobachtung Rechnung, dass nicht alles technisch Mögliche auch gesellschaftlich gewünscht ist, so dass der technische Schutz unter Berücksichtigung gesellschaftlicher Randbedingungen geschehen soll.

Auf technischer Ebene geht es um die Modellierung eines kostengünstigen, reliablen und validen Systems für Gefahrenerkennung und Krisenmanagement, das den Mehrwert der technischen Innovation erkennen lässt und von den Nutzern nicht als Bedrohung wahrgenommen wird. Der Clou der Projektidee liegt darin begründet, dass durch die Verwendung von Infrarotsensoren anstelle von kostengünstigen optischen Sensoren zwei Fliegen mit einer Klappe geschlagen werden können. Denn neben der Reduzierung von Materialkosten wird durch die Verwendung von niedrig auflösenden Kameras auch der Eingriff in die Privatsphäre der Nutzer minimiert, da relativ abstrakte Wärmebilder ausreichen, um die Dichte von Menschenmassen zu detektieren. Es werden somit nur abstrakte Dichtekarten für die Detektion verwendet, die somit auch nicht im Nachhinein in eine höhere Auflösung rücktransferiert werden können, was mögliche Eingriffe in die Privatsphäre über Umwege ermöglichen würde. Mögliche Datenschutzprobleme wurden also bereits bei der Entwicklung der Sensortechnologie mitgedacht, was der Idee des *privacy by design* entspricht.

Da Transparenz bei Technologien, die potenziell als Überwachungstechnologien interpretiert werden können, einen elementaren Aspekt darstellt, wurde auch hierauf besondere Rücksicht genommen. Das innerhalb des SAFEST-Projektes entwickelte Betriebssystem ‚RIOT', welches unter anderem als Plattform für das Internet der Dinge dienlich sein kann, ist komplett offengelegt, was es etwa von anderen Systemen wie ‚Android', wo dies nicht vollständig der Fall ist, unterscheidet. Ein weiterer Vorteil von RIOT ist, dass es selbst auf pfenniggroßen Objekten funktioniert.

Die sozialwissenschaftliche Begleitstudie des Projektes SAFEST bewegt sich in erster Linie im Bereich der (Technik-)Akzeptanzforschung. Primäres Ziel dabei ist die Erstellung einer Akzeptanzstudie, um elementare Faktoren und Dimensionen von Akzeptanz in Bezug auf Sicherheitsmaßnahmen und -technologien am Flughafen offenzulegen und diese in Beziehung zu setzen, wobei hieran angelehnte Fragestellungen durchaus Berührungspunkte mit anderen Themenfeldern aufweisen. So ist die Thematisierung von Akzeptanz im Kontext von Sicherheitsmaßnahmen am Flughafen eng mit Überlegungen wie sie innerhalb der *surveillance studies*, der Risikowahrnehmungsforschung oder der Forschung zu Sicherheitskulturen angestellt werden, verbunden.

Die Struktur der sozialwissenschaftlichen Begleitforschung folgt dabei einem dreiteiligen Aufbau, der auf methodischer Ebene dem Prinzip der Triangulation folgt. So werden hinsichtlich der Analyse der Akzeptanz seitens der Flugpassagiere sowohl qualitative (problem-zentrierte Interviews) als auch quantitative Verfahren (standardisierte Befragungen) eingesetzt. Auf diese Weise wird versucht die jeweiligen Nachteile der einzelnen methodischen Herangehensweisen durch interpretative Rückbezüge und einer damit einhergehenden nicht isolierten (methodischen) Betrachtung des Forschungsfeldes zu reduzieren. Der Passagierbefragung war zudem eine Expertenbefragung mit Experten der Flughafensicherheit des Flughafens Berlin Brandenburg vorgelagert. Im Ergebnis zeigten sich unterschiedliche Präferenzen sowohl zwischen als auch innerhalb dieser Stakeholder.

So deuteten die 15 Experteninterviews darauf hin, dass sich Flughafensicherheit in einem Spannungsfeld zwischen *aviation* (Transport) und *non-aviation* (Ökonomie) bewegt. Interessanterweise wurde der durchaus nicht zu vernachlässigende symbolische Wert mancher Sicherheitsmaßnahmen von den Experten nur am Rande thematisiert, was möglicherweise mit einem eher rational-technischen Verständnis von Sicherheit einhergehen könnte. Dieser Perspektive entspricht auch die geäußerte Tendenz der Experten soziale und rechtliche Nebeneffekte in erster Linie über technische Innovationen lösen zu wollen. Ebenfalls in diesem Lichte ist die von den Experten konstatierte Irreversibilität der Entwicklung der Sicherheitsmaßnahmen (in Form einer ‚Reduktion des Sicherheitsstandards') zu sehen. Ein weiterer Aspekt war das potenziell problematische Verhältnis von etablierten Organisationsstrukturen und neuen technischen Systemen, das vor der Implementierung neuer technischer Systeme mitgedacht werden sollte.

Die problem-zentrierten Interviews mit Flugpassagieren in Schönefeld gaben Aufschluss darüber, dass Akzeptanz unterschiedliche Ausprägungen aufweist. Eine reflektierende Akzeptanz als eine solche mögliche Ausprägung, also eine Akzeptanz, die nach Abwägung der verfügbaren Informationen die Sicherheitsmaßnahmen in ihrer Gesamtheit aktiv bejaht, konnte in den Interviews nicht beobachtet werden. Stattdessen zeigten sich vielmehr Einstellungsmuster, die auf ‚Toleranz'. ‚Ignoranz' und ‚Resignation', also auf passive Formen der Akzeptanz, hindeuteten. Dass Akzeptanz als multidimensionales Konstrukt betrachtet werden sollte, zeigte die Nennung einer Vielzahl an Faktoren, welche die Akzeptanz der Sicherheitsmaßnahmen generell bedingen, wobei der Schutz der Privatsphäre nur ein Aspekt unter vielen war. Andere Aspekte, die in Bezug auf die Ausgestaltung der Sicherheitsmaßnahmen genannt wurden, waren etwa: Transparenz, Diskriminierungspotenzial, Sinnhaftigkeit oder Kosten.

Der Fragebogen der quantitativen Passagierbefragung, der auf den Erkenntnissen der problemzentrierten Interviews basierte, beinhaltete folgende Frage-/Themenblöcke:

- Generelle und spezielle Wahrnehmungen und Einstellungen zu Videoüberwachung
- Sicherheitsempfinden am Flughafen
- Fluggewohnheiten der Befragten
- Vertrauen in bestimmte Sicherheitsakteure
- Subjektive Einschätzungen zu den Sicherheitsmaßnahmen am Flughafen
- Sozio-demographische und sozio-strukturelle Informationen

Die Ergebnisse der Befragung lassen zwar auf eine mehrheitliche Akzeptanz der Sicherheitsmaßnahmen am Flughafen schließen, allerdings ist quantitativ nur schwer erfassbar, welche Ausprägung von Akzeptanz gemeint ist und was sich dahinter verbirgt. Deshalb soll in einem nächsten Analyseschritt eine Rückbindung der Beobachtungen an die qualitativen Interviews erfolgen. Weitere empirische Ergebnisse waren etwa, dass das Alter positiv mit der Akzeptanz korreliert, genauso wie das Vertrauen in die Sicherheitsakteure des Flughafens. Dagegen korreliert die Flughäufigkeit negativ mit der Akzeptanz. Es lassen sich insgesamt zum Teil erhebliche Gruppenunterschiede feststellen, was die Frage aufwirft, wie Flughafensicherheit so organisiert und umgesetzt werden kann, dass diese sowohl aus funktional-technischer und ökonomischer Perspektive als effektiv und effizient als auch aus sozialer und ethischer Sichtweise transparent, freiheitsbewahrend und gerecht ist.

4.5 Neue Technologien – Zukunft der Videoauswertungssysteme

Dr.-Ing. Markus Müller, Fraunhofer IOSB

Das Fraunhofer IOSB als mitgestaltende Institution im Bereich der Zukunft von Videoauswertungssystemen hat sich auf die Bereiche der Optronik, Systemtechnik und Bildauswertung spezialisiert. Optronik bezeichnet dabei elektrooptische Systeme und Verfahren zur Signal- und Bildgewinnung vom Ultravioletten bis zum thermischen Infrarot, während das Feld der Systemtechnik die Fähigkeit der Analyse, des Verständnisses, der Modellierung, der Entwicklung und Beherrschung komplexer Systeme repräsentiert. Die Bildauswertung bezieht sich dabei auf die Aufbereitung, Echtzeitverarbeitung sowie automatische und interaktive Informationsgewinnung aus Bildern und Videos. Eine Reihe von aktuellen Technik-Trends – wie *Big Data*, *Cloud Computing*, *Smart Assets*, *Megacities*, *mobile Apps*, das *Internet of Things* oder *Privacy* – wurden hierbei als potenzielle Anknüpfungspunkte für das Themengebiet der automatisierten Auswertungssysteme gesehen.

Auf Seiten der technischen Entwickler von Videoüberwachungssystemen scheint teilweise auch Konsens darüber zu herrschen, dass Videoüberwachung keine Straftaten verhindert, aber als Unterstützung bei der Strafaufklärung dienlich sein kann. So wurden statistisch gesehen im Jahr 2014 in Berlin 2.965 Gewalttaten begangen, wobei ca. 1.500 Tatverdächtige ermittelt werden konnten. Von diesen Tatverdächtigen konnten gemäß der angeführten Statistik 511 Personen durch die Sichtung von Überwachungsvideos identifiziert werden. Weiterhin wurde der Aspekt der Abschreckung genannt und

in diesem Zusammenhang auf das Beispiel von rückläufigen Vandalismus-Schäden bei den Berliner Verkehrsbetrieben verwiesen, die im Jahr 2008 noch 9,7 Millionen Euro betrugen, während sich die Schäden für das Jahr 2014 auf ca. 4 Millionen Euro reduzierten.

Natürlich besteht aber auch aus Entwicklerperspektive ein Bewusstsein hinsichtlich möglicher Nebenfolgen von Videoüberwachung auf sozialer und rechtlicher Ebene. Neben Problemen mit dem Datenschutz ist das Thema der Transparenz deshalb Teil der entwicklungsstrategischen Agenda. Transparenz bezieht sich dabei etwa auf Fragen wie: Wer nimmt Material auf? Wird dieses Material gespeichert? Wenn ja, wie lange sind die Speicherungsfristen? Was wird aufgenommen? Wer wertet welches Material wie aus? Hinsichtlich der Frage der Akzeptanz von Videoüberwachung wurde auf eine BVG-Studie verwiesen, die zum Ergebnis kommt, dass 84 Prozent der Fahrgäste Videoüberwachung als »eher gut« bis »sehr gut« bewerten.

Es wurde zudem darauf aufmerksam gemacht, dass das Videobild selbst zur Alarmierung nicht zwingend notwendig sei und abstraktere Darstellungsformen – wie etwa das Strichmännchen beim Körperscanner – hier für die Funktionserfüllung ausreichend wären. Die Aktionserkennung und Rekonstruktion der Bewegungsabläufe (hochfrequentes Bewegungsverhalten) ergibt hierbei ein Muster, das eine Normabweichung nahelegt und dann letztlich von den Betreibern weiter ausgewertet werden kann. Aus Datenschutzaspekten wäre es außerdem am besten, wenn ein schwarzer Bildschirm die Grundeinstellung wäre und nur im Alarmfall Strichmännchen gezeigt würden, welche auf abstrakter Ebene dann Bewegungsmuster abbilden. Auch technisch wäre das unproblematisch, denn das eigentliche Videobild braucht der Rechner lediglich zur Berechnung, die Darstellung des Bildes an sich wird dann nicht weiter benötigt. Ausgangspunkt für die Konstruktion von Auswertungstechniken sind dabei immer realweltliche Probleme, wie z. B. Gewalt. Solche Phänomene werden dann dem Versuch der Reproduktion unterzogen mit dem Ziel so eine Situation möglichst realistisch zu simulieren, um die Trefferquote bei der Detektion dieser Phänomene zu maximieren.

Neben einer solchen Abstraktion von Bewegungsabläufen wurde auf diverse andere Verfahren und Möglichkeiten in der Bildgenerierung, -bearbeitung und -auswertung eingegangen, die im Bereich der Videoauswertesysteme Anwendung finden. Die ‚Gated Viewing'-Kamera kann etwa durch Rauch, Scheiben, Regen und Schneefall ‚hindurchschauen', was zum Beispiel bei Bränden besonders relevant werden kann. Außerdem ist dieser Kameratypus auch in der Nacht anwendbar. Als Verfahren der Videooptimierung wurde die Methode der Superresolution erläutert, wodurch sich störende Faktoren ausblenden lassen und das Bild zugleich in höherer Qualität erscheint. Diese Methode unterstützt beispielsweise die Arbeit mit Fahndungsfotos oder einer Nummernschilderkennung. Falls auch hierbei Verfahren eingesetzt werden sollen, die dem Schutz der Privatsphäre Rechnung zollen, kann etwa auf die sogenannte ‚Multi-Frame Super-Resolution' zurückgegriffen werden. Diese basiert auf der Idee Videobilder durch nachträglich eingefügte Pixeleffekte zu abstrahieren, so dass der Schutz der Privatsphäre durch die Anwendung des Frames auf einen festgelegten Bereich gesteuert werden kann. Der sichtbare Bereich kann vordefiniert, alles außerhalb dessen geschwärzt werden. Zudem kann, sofern das Interesse nicht auf der Identifikation von Personen liegt, sondern lediglich auf der Detektion von Bewegungsmustern. Zusätzlich besteht die Option Aufnahmen von Personen zu verpixeln, um diese unkenntlich zu machen.

Wenn man die Perspektive umdreht und positive Facetten von Überwachung thematisiert, kann man Überwachungstechnik auch als Dienstleistung beschreiben, die es Menschen ermöglicht sich freiwillig z. B. beim Betreten bestimmter Infrastrukturen überwachen zu lassen, um sich sicherer zu fühlen und auf diese Weise ggf. ein Eingreifen in kritische Situationen zu ermöglichen. Neben diesem ‚Zukunfts-szenario' sind andere Detektionstechniken bereits Realität. So existiert eine Tattoo-Datenbank zur Identifizierung von nicht identifizierbaren Personen, die Bestandteil eines EU-Projektes war und auf die Organisationen wie Interpol oder das Bundeskriminalamt zurückgreifen können. Die Datenbank macht einen Abgleich von Video-/Bildmaterial mit bestimmten Referenzobjekten. Die darauf basierende Identifizierung von Personen durch körpereigene Modifikationen wurde am Beispiel von tätowierten Leichen und Leichenteilen erläutert.

Dass Videoüberwachung aber nicht nur für forensische oder kriminalistische Aspekte von Interesse ist, sondern auch im Katastrophenfall einsetzbar, zeigte das Beispiel von bestimmten Gefahrenlagen, etwa mit Chemikalien. So könnte der Einsatz solcher Technologien nach der Explosion in einem Chemiewerk die Ortung von vermissten Personen verbessern oder Flugdrohnen zur Generierung von Lagebildern eingesetzt werden, um Vermisste zu finden oder Gefahrenquellen zu erkunden. Auch der Einsatz von Robotern für solche Zwecke wurde mit dem Argument, dass somit keine Menschenleben auf das Spiel gesetzt werden, angeführt. Somit sind die Bereiche der Flugrobotik, Landrobotik und Sensorik für Entscheidungsträger als Hilfsmittel zur Entscheidungshilfe einsetzbar, um dadurch bestimmte Situationen für Entscheidungsträger beherrschbar zu machen. Andere Einsatzbereiche für Videoüberwachung finden sich in der ‚medicine care'. Die Überwachung von Personen, die beispielweise aus dem Bett fallen und sich nicht mehr eigenständig helfen können, wurde in diesem Zusammenhang erwähnt.

Als treibender Faktor, der Entwicklungen aller Art im Bereich der Videoüberwachung forcieren wird, wurde der Konkurrenzkampf auf Produzentenseite genannt, der dazu führe, dass innovative technische Lösungen immer verfügbarer, hochwertiger und gleichzeitig günstiger in der Anschaffung werden. Zusammenfassend lässt sich die Zukunft von Videoauswertesystemen aus Entwicklerperspektive demnach auf einer Optimierung der Gewährleistung von Datenschutz und Transparenz in einer stetigen Leistungsverbesserung bei immer geringeren Kosten verstehen.

4.6 Überwachung und Datenschutz im öffentlichen Raum

Dr. Rainer Stentzel, Bundesministerium des Innern

Aus der Perspektive einer Bundesbehörde lässt sich Überwachung als Phänomen an der Schnittstelle zwischen Politik und Gesetzgebung verorten. Der Vortrag von Dr. Rainer Stentzel war somit weniger technisch angelegt als der seines Vorredners und fokussierte eher auf das Verhältnis von Datenschutz und Öffentlichkeit, die Überwachung öffentlicher Räume sowie der Konstruktion von Sicherheit aus rechtlicher Perspektive.

Als Ausgangpunkt wurde auf das Rechtsgebiet des Datenschutzes eingegangen, das einerseits zwar hoch entwickelt ist, als Schutzgut aber teilweise fehlinterpretiert wird. Außerdem wird der Datenschutz in der Wahrnehmung einiger Bürger bekanntlich zunehmend zugunsten anderer Argumentationen und

Sicherheitsdiskurse beschnitten. Im Datenschutzrecht lässt sich derzeit eine Systematik erkennen, die sich in dem Anspruch an eine hohe Regelungsdichte von und an Technik äußert, so dass technische Prozesse der Kommunikationsverarbeitung immer mehr zu einem juristischen Gegenstand werden.

Die Frage, was es zu schützen gilt, also was ein Schutzgut darstellt, lässt sich dabei mit Rückgriff auf die sogenannte Sphärentheorie beantworten, welche im Wesentlichen im Zivilrecht angelegt ist. Diese unterscheidet zwischen der Intimsphäre, der Privatsphäre und der Öffentlichkeit, wobei letztere nochmal räumlich und sozial zu differenzieren ist. Der Anspruch des Individuums auf Grenzziehung ist hier verankert mit dem Ziel, private Informationen der Öffentlichkeit gegenüber (punktuell) vorenthalten zu können und nicht umgekehrt, also in Form einer wie auch immer gearteten Rückholung von privaten Informationen, was für den Bereich der Privatsphäre gemäß dem Vortragenden allerdings gerade der Fall ist, wenn sich die Öffentlichkeit auf immer mehr Räume erstreckt.

Wichtig in diesem Zusammenhang ist die Tatsache, dass das Datenschutzrecht – als Abstrahierung des Rechtes auf Privatsphäre – ein öffentliches Recht darstellt, was bedeutet, dass der Staat gegen und auch ohne den Willen von Betroffenen durchsetzt. Die staatliche Machtposition spiegelt sich auch im Recht der informationellen Selbstbestimmung wider, das sich nie wirklich durchgesetzt hat und in den Bürgerprotesten zur Volkszählung in den 80er Jahren verwurzelt ist. Das Verhältnis zwischen Staat und Bürger sollte hierdurch klarer geregelt werden. Es entspricht somit der Neuregelung des Staat-Bürger-Verhältnisses, bei dem es nicht um die individuelle Selbstbestimmung zum Umgang mit persönlichen Informationen geht, sondern um die Behandlung durch den Staat.

Der öffentliche Raum hat eine zentrale Bedeutung für die Grundrechtsausübung. Im öffentlichen Raum darf man sich frei bewegen und auch Empfangen und Senden von Information im öffentlichen Raum ist elementar für die Gewährleistung von Grundrechten. Wird aber der öffentliche Raum bedroht, zum Beispiel durch die Eigeninteressen Privater oder den Staat, der sich bedient, selektiert und repressiv agiert, sind diese Grundrechte in Gefahr. Hierbei kann auch der Datenschutz als relativ neue Bedrohung bewertet werden, da er mit seinem allumfassenden Regelungsanspruch dem Einzelnen nicht nur ein Recht, sondern auch staatliche eine Sanktion an die Seite stellt, nämlich wenn der Staat versucht seine Rechte durchzusetzen. Der öffentliche Diskurs um das Recht auf Vergessen werden reagiert gewissermaßen auf diesen Sachverhalt.

Ein weiterer Aspekt, der sich im Zusammenhang mit der Öffentlichkeit auftut, sind die sogenannten *chilling effects*, die in zwei unterschiedliche Richtungen gedeutet werden können. Eine Interpretationsweise folgt dabei dem Bundesverfassungsgericht, das in diesem Zusammenhang von einem diffusen Gefühl von Überwachung spricht. *Chilling effects* können aber auch andersherum ausgelegt werden, wenn etwa der öffentliche Raum nicht mehr als solcher nutzbar ist, wenn also mehr Schutz durch den Staat notwendig ist, was zum Beispiel durch Terrorismus der Fall sein könnte. Auf das Internet bezogen darf der Nutzer durch die staatliche Interpretation von *chilling effects* also auch nicht das Gefühl bekommen, ständig überwacht zu werden, was diesen Effekten einen gewissen Steuerungs-charakter verleiht.

Hinzu kommt die Streubreite von Überwachung, wie sich am Beispiel der Vorratsdatenspeicherung erkennen lässt. Hier stellt sich die Frage nach Quantität und Eingriffstiefe, wenn geprüft werden muss,

wie viele Personen aus welchen Gründen überwacht werden und von staatlichen Repressionen betroffen sind.

Die Frage wie man die Öffentlichkeit absichern und schützen kann und wann eingegriffen wird, ist Abwägungssache und Einzelfallabhängig, so dass hierbei keine *a priori*-Entscheidungen existieren. Das bedeutet, dass ein demokratisch legitimierter Gesetzgeber verantwortlich ist, dies im Einzelfall zu prüfen, wenn zum Beispiel mehr Polizei oder Technologie eingesetzt werden sollen. An dieser Stelle ist der internationale Vergleich interessant, da *chilling effects* auf der Länderebene im öffentlichen und medialen Diskurs oftmals ganz unterschiedlich interpretiert und wahrgenommen werden.

Wenn man also Fragen des Datenschutzes oder der informationellen Selbstbestimmung als Auftrag und Abwägungsentscheidung des Staates begreift, dann ist der vorgelagerte demokratische Diskurs wichtig sowie die Art und Weise der Entscheidungsfindung. Dieser Diskurs ist durchaus als Voraussetzung anzusehen und sollte vor allen Dingen die Möglichkeit auf Öffentlichkeit ins Zentrum der Aufmerksamkeit rücken und nicht zwangsläufig datenschutzrechtliche oder sicherheitsrelevante Fragen.

Soll die Bedeutung der Öffentlichkeit also ernst genommen werden, sind Gewinne und Verluste von Eingriffen offenzulegen und Negativfolgen zu minimieren (z. B. rechtlich oder technisch). Hierbei sollte ein gewisses Feintuning beachtet werden, um nicht punktuell und stetig die Sicherheit zu erhöhen und somit immer weiter zu regulieren. Denn Deregulierung ist immer schwieriger als Regulierung, das gilt auch für den Datenschutz.

5. Paneldiskussion

Teilnehmer: Dr. Ulrich Meissen, Fraunhofer FOKUS
Dr. Nils Zurawski, Universität Hamburg
Gerold Reichenbach, MdB, SPD Bundestagsfraktion
Nina Warken, MdB, CDU Bundestagsfraktion
Dr. André Hahn, MdB, Bundestagsfraktion DIE LINKE

Moderation: Konrad Litschko, taz Redakteur Themenbereich Innere Sicherheit

Nach den Terroranschlägen in Kopenhagen und Paris entfachte auch im Deutschen Bundestag erneut die Debatte um die Konsequenzen, die aus diesen Ereignissen gezogen werden müssen. Eine Verschärfung der Sicherheitsgesetze wird diskutiert, die Vorratsdatenspeicherung ist wieder auf der Agenda, auch die Decodierung von Verschlüsselungstechniken und die Sicherung von Fluggastdaten werden in Betracht gezogen und somit rückt auch das Thema des Workshops, nämlich die „Überwachung im öffentlichen Raum“, in den Fokus der Politik.

Die Vorfälle in Paris und Kopenhagen haben gezeigt, dass die Täter durch die Vorratsdatenspeicherung zwar bekannt waren, die Taten aber nicht verhindert werden konnten. In den Vereinigten Staaten und Großbritannien konnten Anschläge nicht verhindert werden, obwohl die dortigen Geheimdienste über weit mehr Rechte verfügen als in Deutschland. Es müssen also neue Fragen aufgeworfen werden; Fragen nach den Maßnahmen, die nicht ergriffen wurden. Die Vergangenheit hat gezeigt, dass die Speicherung von Daten zur Aufdeckung von kriminellen Netzwerken sinnvoll sein kann, konkrete Ergebnisse zur Verhinderung konnten aber nicht erzielt werden. In Deutschland ist die NSU-Affäre ein gutes Beispiel dafür, dass falsche Fragen zu unnützen Ergebnissen führen. Das Wissensmanagement zwischen Behörden greift offensichtlich nicht ineinander, wenn Informationen an verschiedenen Stellen vorliegen, aber die Zusammenhänge nicht hergestellt werden.

Die Politik muss neue Wege gehen

An diesem Punkt kommen wir zu dem vieldiskutierten Phänomen der Symbolpolitik. In Extrem-situationen wie akuter Terrorgefahr ist das Sicherheitsbedürfnis der Bürger sehr groß. Die Politik befindet sich in einer Zwickmühle, da sie es sich nicht erlauben kann, keine Antworten zu präsentieren. Gesetze, die im Nachgang konkreter Ereignisse im Schnelldurchlauf entworfen wurden, sind später aber auch im alltäglichen Leben anwendbar und können zu extremen Einschränkungen der bürgerlichen Freiheiten führen.

Eine vollständige Überwachung von „verdächtigen“ Personen oder Personengruppen kann so oder so personell nicht geleistet werden. Es wird daher immer wichtiger, die Zusammenarbeit zwischen den Behörden zu optimieren und ihnen Instrumente an die Hand zu geben, mit denen schneller und effektiver reagiert werden kann. Die Aufhebung des Bankgeheimnisses z. B. ist ein Tabu, dabei wäre die Aufdeckung von Geldflüssen ein effektiver Weg zur Bekämpfung von organisierter Kriminalität und deren Verquickung mit dem internationalen Terrorismus.

Theoretisch wird in Zeiten von Smart Phone und dem Internet der Dinge eine permanente Überwachung schon bald möglich sein. Daten können anlasslos gesammelt und im Hintergrund verwertet werden. Es handelt sich dabei nicht mehr nur um Telefondaten, die Digitalisierung dringt in alle Lebensbereiche vor. Provokant gesagt, könnte man jeden Bürger mit einem Chip ausstatten und so jeden Terroristen zumindest nach der Tat fassen.

Mit dem Wissen um diese Möglichkeiten, müssen daher die gesetzlichen Schranken zur Auswertung erhöht werden. Der Europäische Gerichtshof ging hier voran, indem er die anlasslose Vorratsdatenspeicherung als Verstoß gegen die Grundrechte der EU Bürger proklamierte[2].

Ist Technik per se verdammungswürdig?

Das wäre der falsche Schluss, es darf vor allem keine Scheindiskussion zu Technikrisiken geführt werden. Der Nutzer sollte sich nicht bange machen lassen und sich gut über Risiken beim Gebrauch technischer Geräte informieren. Mittlerweile bekommt man schon Angst vor seinem Smart Phone, benutzt aber seit Jahren eine Kreditkarte, ohne sich über die immensen Datenmengen, die bei Kreditkartenkäufen abgefragt werden, und deren Verwertung Gedanken zu machen.

Bereits heute hat fast jeder ein Smartphone, mit dem unendliche Mengen an Daten gesammelt werden. Es ist nicht unwahrscheinlich, dass wir in der Zukunft die Überwachungskameras selbst mit uns herumtragen, man denke nur an Google Glass. Problematisch ist, dass die Technologie schneller ist als die Schiedsrichter und die Spielregeln schon nicht mehr verstanden werden. Das birgt ein sehr hohes Missbrauchspotential.

Technik schafft auch Realitäten. Die private Datensammlung über Payback-Systeme, Smart Phone oder Kreditkarte hat eine größere Bedeutung als die staatliche. Viele Menschen kapitulieren vor der Komplexität der digitalen Welt und versäumen sich und ihre Daten zu schützen.

Die Diskussion mit der Technologie muss offen geführt werden. Daher darf sie auch nicht verteufelt werden, weil sonst keine Transparenz möglich ist. Die Technologie kann nicht nur dafür sorgen, immer mehr Daten zur Verfügung zu stellen, sie kann auch helfen, den Einsatz dieser Daten zu reglementieren. Am Beispiel Überwachungskameras könnte das z. B. heißen, dass die Kamera keine Personenerkennung zulässt und so die Privatsphäre des Einzelnen geschützt wird. Es können auch Technologien entwickelt werden, die verhindern, dass Daten im Hintergrund ohne Wissen des Bürgers gesammelt werden. Die gesetzgeberischen Möglichkeiten müssen in diesem Bereich voll ausgeschöpft werden, um die Freiheitsrechte der Bürger zu schützen.

Es muss dahingehend ein Umdenken stattfinden, wie man den Bürger vor zu viel Überwachung und Datenklau schützen kann. Die Verhältnismäßigkeit zwischen Schutz der Freiheit und anlassloser Überwachung der Bürger muss gewahrt werden. Die Forschung geht immer nur in die eine Richtung, mehr Technik, mehr Überwachung, die zu mehr Sicherheit führen soll. Wieviel Freiheit sind wir aber bereit für unsere Sicherheit zu opfern, denn die Erfahrung zeigt, dass ein Zurückfahren bereits implementierter Sicherheitstechnik in den seltensten Fällen stattfindet und so der

[2] siehe http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157de.pdf [30.03.2015]

Überwachungsapparat immer weiter anwächst. Grundsätzlich gehen wir aber davon aus, dass nichts unabänderlich ist, schon gar nicht, wenn es um gesellschaftliche Prozesse geht, wie man an der Energiewende sieht.

Lohnenswert wäre es sicher, in der Zukunft vermehrt über Lösungen außerhalb des Technikbereichs nachzudenken und das finanzielle Engagement in dieser Richtung zu erhöhen. Letztendlich werden Menschen unter Menschen gesucht und der Algorithmus kann nicht flexibel genug reagieren. Wir brauchen neue Denkrichtungen, um die Spirale von immer mehr Sicherheit durch immer mehr Technik zu stoppen.

Welche Ansätze können wir verfolgen, um einen wirksamen Schutz gegen Terroranschläge zu entwickeln und gleichzeitig die Freiheitsrechte der Bevölkerung zu schützen? Um hier einen Schritt weiter zu kommen, müssen die Verbindungen zwischen der Industrie, die die Sicherheitstechnik herstellt, und der Politik transparenter werden. Ein weiterer entscheidender Schritt wäre das Offenlegen von Geldflüssen, durch die der internationale Terrorismus finanziert wird. Wenn es um das Bankgeheimnis im Gegensatz zum Datenschutz geht, wird schnell klar, dass verschiedene Interessensgruppen bestehen, die unterschiedlichen Einfluss nehmen können.

Die große Frage lautet letztendlich: Hat die Politik überhaupt noch das Heft in der Hand, wenn es um den Schutz der Bürger geht oder sind die privaten Datensammler im Vorteil?

6. Schaufenster Sicherheitsforschung

Erstmalig ließ sich im Rahmen des Workshops das neue *Schaufenster Sicherheitsforschung* – gestaltet in Zusammenarbeit mit Fraunhofer Fokus / Innovationszentrum Öffentliche Sicherheit und dem Forschungsforum Öffentliche Sicherheit – besichtigen, das die komplexe Verzahnung von Technik und Gesellschaft plastisch macht. Das Schaufenster als interaktiver Demonstrationsraum bietet die Möglichkeit Innovationen in Hinblick auf das Zusammenspiel von technischen Möglichkeiten und ihren vielfältigen Implikationen zu untersuchen.

Besichtigung des *Schaufenster Sicherheitsforschung* während des Workshops

Fotos: C. Frickemeier

Das Schaufenster Sicherheitsforschung leistet einen Beitrag zu einer besseren Dissemination, Vernetzung und Verwertung von Forschungsergebnissen der Sicherheitsforschung. So konnten folgende sechs Projekte aus dem BMBF-Förderprogramm der Hightech-Strategie inhaltlich in den Workshop eingebunden werden: ASEV, CamInSens, Critical Parts, FluSs, MUVIT, SAFEST, SIRA.

Das Schaufenster ist ein Ort für Entscheidungsträger aus Politik und Wirtschaft, um die Potentiale der Ergebnisse der Sicherheitsforschung besser zu erkennen (Format: Führungen für politische Delegationen, Hosting von Veranstaltungen von Verbänden und Gremien mit Führungen, etc.). Darüber hinaus versteht sich das Schaufenster als interdisziplinäre Plattform, um Forschungspartner, Wirtschaft und Endanwender sowie politische Schlüsselpersonen an konkreten Beispielen diskutieren zu lassen, zu vernetzen, Probleme zu formulieren und neue Ideen entstehen zu lassen (Format: Workshops, Konferenzen, Fachtagungen, etc.).

Die präsentierten Ergebnisse werden nicht nur temporär, sondern langfristig in den Demonstrationsraum implementiert, so dass ein lebendes Projektarchiv entsteht. Der Demonstrationsraum wird regelmäßig von nationalen und internationalen Fachgruppen, Entscheidern in Behörden, Wirtschaft, Politik und Medienvertretern besucht. Auf diese Weise wird sowohl ein Dialog zwischen Wissenschaft, Politik und Unternehmen als auch der interessierten Öffentlichkeit initiiert und die Vernetzung sowie die Entstehung von Synergien gefördert. Insbesondere gegenüber Politikern wird eine unmittelbare

Erlebbarkeit der Forschungsergebnisse und technischen Innovationen der zivilen Sicherheitsforschung, die über den Fachdialog innerhalb der Sicherheitsforschung hinausgehen, ermöglicht.

7. Ergebnisse der Arbeitsgruppen

7.1 AG I: Soziale und ethische Implikationen von Überwachungstechnologien

Moderation: Dr. Benjamin Rampp, Universität Trier & Gabriel Bartl, Freie Universität Berlin

Inhaltliche Schwerpunkte

Der Fokus der Arbeitsgruppe I lag auf sozialen und ethischen Implikationen von Überwachungstechnologien. Insgesamt schwebte den Moderatoren ein bewusst offen gehaltener, explorativer Zugang zur Thematik vor, was umso mehr ein Abstecken des Diskussionsrahmens erforderte, um die breit angelegten Debatte um Überwachung auf bestimmte Inhalte einzugrenzen, so dass bis zu einem gewissen Grad zu berücksichtigende Aspekte vorgegeben wurden.

Als Referenz der Diskussionen einigte man sich auf einen Überwachungsbegriff, der sich v. a. auf Videoüberwachung und automatisierte Mustererkennung beziehen sollte. Die Diskussion sollte sich allerdings nicht nur darauf konzentrieren, wie Überwachung und die dazugehörigen Technologien eine Gesellschaft verändern, sondern genauso andersherum auf die Frage, inwieweit technische Innovationen auf soziale Bedarfe reagieren.

Durch die Übernahme dieser Perspektive wurde demnach keine Kausalrichtung im Beeinflussungsverhältnis zwischen Entwicklungsprozessen im Bereich von Überwachungstechnologien auf der einen Seite und Gesellschaft auf der anderen Seite für die Diskussion als wichtiger erachtet; vielmehr wurde der Rahmen absichtlich so gesetzt, um die Komplexität wechselseitiger Interdependenzen explizit berücksichtigen zu können. Denn wie bereits der Vortrag von Eric Töpfer gezeigt hatte, ist die Durchsetzung und die Anwendung von Innovationen immer von sozialen Interpretationsleistungen abhängig, was unter anderem zur Fragestellung überleitete, wie neutral Technik überhaupt sein kann. Bezogen auf die Sichtweise, dass Technik auf Gesellschaft wirkt, wurde außerdem zu Beginn der Vorschlag gemacht, die ambivalente (und oftmals nicht intendierte) Dynamik von Nebenfolgen, die durch Überwachung produziert werden, in die Arbeitsgruppen-Diskussion zu integrieren.

Insgesamt wurden innerhalb der Arbeitsgruppe drei Bereiche identifiziert, die tiefergehend erörtert wurden: 1. Vertrauen, 2. Normalitätsvorstellungen, 3. Identifikation und Ablehnung. Wie diese drei Themencluster mit Überwachung in Verbindung gebracht wurden soll nachfolgend erläutert werden.

Vertrauen

Zentral für die Erörterung des Phänomens Vertrauen im Zusammenhang mit Überwachung war die Frage, wer die Träger und Adressaten von Vertrauen sein können. Generell lassen sich hierbei verschiedene Akteure identifizieren, wie etwa die Entwickler oder die Nutzer solcher Technologien. Auf der Seite der Nutzer finden sich auf staatlicher Seite z. B. Behörden, Organisationen oder Institutionen und auf privatwirtschaftlicher Seite Unternehmen. Außerdem lassen sich je nach Perspektive die überwachten Subjekte als Nutzer, aber genauso als Betroffene von Überwachung benennen. Diese Differenzierung deutet bereits darauf hin, dass zwischen einem Vertrauen *in* die Funktionsweise von Überwachungstechnologien und dem Versuch der Erzeugung von Vertrauen *durch* Überwachung zu unterscheiden ist.

Bei den Diskussionen um Vertrauen in Überwachungstechnologien wurde auch der Aspekt der Technikangst thematisiert, wobei sich nicht alle Teilnehmenden in der Arbeitsgruppe einig waren, ob dieses Phänomen wirklich zu beobachten sei, wenn man sich die Gewöhnungseffekte hinsichtlich der Nutzung und die damit verbundenen Risiken für verschiedenste Technologien ansieht. Der Versuch einer analytischen Differenzierung zwischen Gleichgültigkeit und Vertrauen wurde hierbei als notwendig erachtet, um die beobachteten Phänomene nicht zu verwechseln. In Hinblick auf das Vertrauen in staatliche und private Akteure der Überwachung wurde ein Missverhältnis diagnostiziert, da staatliche Überwacher kritischer betrachtet werden, obwohl fraglich ist, dass von ihnen tatsächlich mehr Bedrohungspotenzial ausgeht.

In Bezug auf die Messung von Vertrauen wurde auf das Problem der Operationalisierung eingegangen. Vertrauen als komplexes multifaktorielles Konstrukt für das je nach Blickwinkel unterschiedlichste Definitionen bestehen ist demnach als Indikator nicht ganz leicht zugänglich zu machen. Wenn man diesen Versuch wagen wollte, müsste man sich also im Klaren darüber sein, auf welche Facetten man fokussiert und welche man bewusst ausblendet. Hierbei gilt es dann auch die Implikationen des Konstrukts in der Interpretation zu berücksichtigen, um nicht die falschen Schlüsse zu ziehen.

Wie die Nutzung von Überwachungstechnologien im Zusammenhang mit Vertrauen zu bewerten ist, wurde ebenso diskutiert. Auf der einen Seite wurde Überwachung – hierbei am Beispiel von ‚Baby-Phones' – als vertrauensfördernd betrachtet. Es wurde an dieser Stelle angemerkt, dass der Versuch Unsicherheiten mittels Technik zu reduzieren zu strukturellen Veränderungen führen kann, die gerade im Kontext von Überwachung in einer Kultur des Verdachts münden können, wenn Abweichungen von der Norm Misstrauen generieren. Ob die Optimierung der Kontrolle von Unsicherheiten als Strategie der Kontingenzbewältigung zielführend ist und stattdessen nicht auch die Akzeptanz und der aufgeklärte Umgang mit diesen Unsicherheiten eine Alternative darstellen könnte, wurde nicht abschließend geklärt. Die Diskussion um Akzeptanz und Normalisierung leitete schließlich auch in das zweite Themengebiet der Normalitätsvorstellungen über, auf das im Folgenden eingegangen werden soll.

Normalitätsvorstellungen

Normalitätsvorstellungen beziehen sich im Zusammenhang der Diskussion auf die Frage, wo der Maßstab zur Bewertung von Überwachung angelegt werden soll. Zum einen sind hier Grenzwerte gemeint, wobei sich diese wiederum in ihren subjektiven und objektiven Ausprägungen unterscheiden können, so dass gefragt wurde, welche der beiden ‚Größen' relevanter ist und wie bei unterschiedlichen individuellen Präferenzen überhaupt ein kollektiver Konsens erzielt werden kann. Da subjektive Wahrnehmungen kontingent und dadurch oftmals paradox sind – wie es etwa Statistiken zu den Einschätzungen von Autofahrern in Bezug auf ihr eigenes Können und das anderer mobiler Verkehrsteilnehmer offen legen – wurde ihre Relevanz in der Vergangenheit zugunsten der Delegation von Entscheidungen an Experten zurückgedrängt; ein Umgang, der sich mittlerweile verändert hat. Denn subjektive Wahrnehmungen können genauso soziale Realität beeinflussen und dies in zum Teil entscheidenderer Weise als vermeintlich objektive Expertenmeinungen. So führt, gemäß dem Thomas-Theorem, jede individuelle Handlung, ganz gleich auf welchen Grundlagen (also subjektiven Konstruktionsleistungen oder ‚objektiven' Realitäten) sie fußt, zu realen Konsequenzen. Bezogen auf

das Thema der Überwachung bedeutet dies etwa, dass der gesellschaftlichen Wahrnehmung von Überwachung und den daraus resultierenden sozialen Effekten mindestens genauso viel Beachtung geschenkt werden sollte wie der tatsächlichen Funktionsweise solcher Technologien. Allerdings ist aufgrund der zunehmenden Komplexität von technischen Systemen und der Intransparenz von Überwachungstechnologien eine Bewertung oftmals nicht möglich, was auf ein Demokratiedefizit hindeutet, wenn der Staat technische Lösungen implementiert, die in ihrer Wirkungsweise für Laien nicht nachvollziehbar sind.

Ein weiterer Aspekt, der im Zusammenhang mit Normalitätsvorstellungen genannt wurde, bezog sich noch stärker auf die potenziellen Auswirkungen von Überwachung. Es wurde geäußert, dass Überwachung die Tendenz einer Gesellschaft konform zu werden möglicherweise befördert. Konformität war hierbei aber nicht ausschließlich negativ konnotiert, da z. B. auf rechtlicher Ebene die Rede vom gleichen Recht für alle durchaus sinnvoll ist. Bezogen auf die soziale Ebene ist Konformität allerdings ein als ambivalent zu deutendes Phänomen, da sie die Vielschichtigkeit und den Pluralismus von Gesellschaften – und damit auch deren Innovationspotenzial – zu untergraben droht. Konformität wurde in diesem Kontext auch als Resultat von Überwachung durch die Etablierung und Durchsetzung von standardisierten Kriterien betrachtet. Denn diese Standardisierungen generieren einen Inklusions-/Exklusions-Mechanismus, der Abweichungen von der Norm mit Ausschluss sanktioniert, wodurch die Tendenz zu konformem Verhalten möglicherweise gestärkt wird.

Die Funktionen von Überwachung wurden außerdem aufgegriffen. Hier konnten erneut zwei konträre Positionen bestimmt werden. Auf der einen Seite wurde Überwachung als notwendiges Kontrollinstrument bestimmt, das die Menschen dazu bringt Regeln einzuhalten, so wie es etwa die Überwachung des Straßenverkehrs zeigt. Diese Position basierte auf der Sichtweise, dass der Staat eine Schutzfunktion innehat, der er mittels Überwachung als Unterstützungs- und Entscheidungshilfe nachgehen kann, so dass der Schutz von potenziellen Opfern den Einsatz von Überwachungstechniken legitimiert. Die Gegenposition fragte, ob wir wirklich überall Überwachung benötigen und ob hier nicht das Gebot der Verhältnismäßigkeit mehr in den Fokus rücken sollte, da Überwachung genauso als potenzielle Bedrohung zu sehen ist. Hier wurde der oben dargestellte Faden wieder aufgenommen, wenn man an die Annahmen von Technik (Algorithmen, Raster; Wer/was ist normal?) und die damit verbundenen Ungleichheiten, die aus Überwachung resultieren, denkt. Verkettungen, die also bis zur Exklusion führen wurden am Beispiel von Paypal-Konten, die aufgrund schlechter Schufa-Scores nicht eingerichtet werden konnten diskutiert. Dass das Zustandekommen solcher Scores im Verborgenen geschieht und für die Betroffenen nicht nachvollziehbar ist, verwies erneut auf die Bedeutung von Transparenz im Kontext von Überwachung.

Auch wenn bestimmte Effekte in der ursprünglichen Konzeption einer Technologie nicht intendiert waren, können sie durch das Phänomen des *function creep* relevant werden. Dieser Terminus beschreibt eine schleichende Funktionsausweitung von Technologien; wenn die ursprünglich intendierte Funktion also nach und nach für andere Zwecke nutzbar gemacht wird (vgl. analog hierzu die Darstellung der Funktionsverschiebung beim Einsatz von BVG-Kameras im Vortrag von Töpfer). Die Verschiebung der Logik der staatlichen wie privatwirtschaftlichen Datensammlung wurde zudem an dem Beispiel, dass nicht das Individuum im Zentrum des Interesses der Überwacher steht, sondern dessen Merkmale,

geschildert. So ermöglicht vor allem die Rekombination von Einzelmerkmalen Rückschlüsse auf die Personenebene, wodurch sich im Vergleich mit früheren Formen eine neue (Wissen-)Form von Überwachung etabliert zu haben scheint.

Die Auffassung, dass Überwachung ambivalent ist, da sie je nach Kontext eine Schutzfunktion hat, aber genauso (oder oftmals auch gleichzeitig) die Einschränkung von Handlungsmöglichkeiten bedeuten kann, leitete zur Frage über, ob solche Technologien wirklich wünschenswert sind und wenn ja, für wen. Normalitätskonstruktionen sollten deshalb durchaus kritisch hinterfragt werden. Mit Blick auf die heutige Gesellschaft, in der viele Leute die Meinung vertreten, dass sie besser nicht darüber nachdenken wollen, welche Daten von ihnen wo gespeichert werden und was damit potenziell angestellt werden kann, wird dieser Aspekt klarer. Somit ist es womöglich nicht ausreichend technische Innovationen im Bereich der Überwachung auf positive und negative Auswirkungen hin zu untersuchen. Vielmehr sollte die Analyse eines Strukturwandels, der auch dadurch bedingt ist, im Zentrum der Analyse stehen, um soziale Veränderungsprozesse und Normalitätsproduktionen nicht aus dem Blick zu verlieren. So deuten die zu beobachtenden strukturellen Veränderungen beispielweise auf ein Missverhältnis hin, wenn von einer Erosion von Vertrauen die Rede ist, das sich auch mit der Expansion von Überwachung erklären lässt. Hinzu kommt eine Zunahme an Selbstüberwachung als Ausdruck von geringem Selbst-Vertrauen und dem Wunsch Kontrollierbarkeit zu generieren. Als Beispiel wurde hierbei die ‚Überwachungsmentalität' bei so manchen Eltern herangezogen, die teilweise sehr stark ausgeprägt ist und somit die Freiräume der Kinder einzuschränken droht.

Der Strukturwandel wurde an zwei weiteren Beispielen aufgezeigt. Erstens für den Fall der Gewöhnung an die sich ausbreitende Nutzung von Smartphones, die anfänglich noch mit Debatten über Strahlenwerte kritisch aufgeladen war. Diese Wirkung verpuffte mit der Zeit, so dass sich die Frage stellt, ob die Überwachungsthematik im Zusammenhang mit Smartphones womöglich bald keine Rolle mehr spielen wird. Ein weiteres Beispiel, das eingebracht wurde, fokussierte auf staatliche Überwachung und Habituation, wenn auf die Proteste gegen die Volkszählung in den 80er Jahren verwiesen wurde, die heutzutage wohl nur noch schwer vorstellbar sind.

Identifikation und Ablehnung

Ein drittes Themenfeld, das innerhalb der Arbeitsgruppe erörtert wurde, bezog sich auf Kosten-Nutzen-Abwägungen im Zusammenhang mit Überwachung. Es stellte sich also die Frage, wer sich inwieweit mit den Entwicklungspotenzialen von Überwachungstechnologien identifizieren kann und wer diese eher ablehnt. Auf der Nutzenseite wurde neben einer gesteigerten Effizienz von Überwachung ein höheres Maß an Objektivität von Videoaufzeichnungen behauptet, welches mit verringerten Beobachtungsfehlern einhergehe. Zudem wurde der ökonomische Nutzen beim Einsatz von technischen Überwachungssystemen für die Sicherheitswirtschaft angeführt. Das Effizienzargument bezog sich dabei auf die Möglichkeit mit optimiertem Ressourceneinsatz ein hohes Maß an Sicherheit generieren zu können. Als Gegenargument wurde angeführt, dass sich gemäß einiger Befragungen mehr Menschen für Überwachung durch Personal als mittels technischer Systeme aussprechen und das subjektive Sicherheitsgefühl durch den Rückgriff auf Technik somit nicht wirklich gesteigert werde. Das gewichtigste Argument auf der Kostenseite war hierbei allerdings die Produktion und Verschärfung

sozialer Ungleichheiten durch die Funktionslogik von Überwachungstechnologien. Beispielhaft wurde die potenzielle Diskriminierung durch Algorithmen, die bestimmte Raster definieren, angeführt.

Versuche Kosten und Nutzen für die Betroffenen gegenüberzustellen, indem etwa nach der Akzeptanz von bestimmten Überwachungstechnologien gefragt wird, sind außerdem mit Vorsicht zu genießen, da auf interpretativer Ebene oftmals nur schwer zwischen Akzeptanz im engeren Sinne und Ignoranz, Toleranz oder Resignation zu unterscheiden ist. Bezogen auf eine effizientere und weitreichendere Wissensproduktion, stellte sich außerdem die Frage, ob mehr Wissen zwangsläufig einen Mehrwert generiere, wenn nicht klar ist wie dieses Wissen kanalisiert und weiterverarbeitet werden kann und welche Pfadabhängigkeiten sich aus bestimmten Wissensformen ergeben. An diesem Punkt wurde dann auch auf die Relativität von Wissen in Bezug auf das Nicht-Wissen am Beispiel der historischen Entwicklung der Physik (Mach und Heisenberg) problematisiert.

Thesen & Empfehlungen der Arbeitsgruppe

Insgesamt einigte sich die Arbeitsgruppe darauf, dass technische Innovationen im Bereich der Überwachung nur schwerlich einer Abwägung aus Vor- und Nachteilen standhalten können, da diese relativ zu betrachten sind. Denn: Verändert sich Gesellschaft, verändert sich auch die Grundlage der Diskussionen. Zentral bleibt somit die Analyse von strukturellen Veränderungen (z. B. Gewöhnungseffekte im Kontext von Überwachung), denn die Auswirkungen des Einsatzes von Technik sind immer ambivalent und somit nur schwerlich in positive und negative Effekte aufzuspalten.

Eine Gesellschaft, in der man besser nicht darüber nachdenkt, welche Daten gespeichert werden und welches Potenzial sich daraus für bestimmte Akteure ergibt, steht exemplarisch für die Notwendigkeit einer öffentlichen Debatte. Diese Debatte verlangt nach politischen Entscheidungen, wobei sich die Frage stellt, welche Gruppen mit welchen Präferenzen in welchem Maße in diese Prozesse involviert werden können und wie sich Entscheidungen legitimieren lassen, die zahlenmäßig großen Minderheiten – aber nicht der absoluten Mehrheit – entgegenstehen. An dieser Stelle wurde auch darauf aufmerksam gemacht, dass Entscheider Verantwortung für die von ihnen getragenen Konsequenzen übernehmen müssen. Von technischer Seite wurde zudem angeregt, dass die Sozialwissenschaften als Ideengeber verstärkt an die Techniker herantreten sollen, um konkrete soziale Probleme aufzuzeigen, die möglicherweise technisch gelöst werden können.

Die Empfehlungen der Arbeitsgruppe bezogen sich darauf, wie zukünftig mit Überwachung umgegangen werden könnte. Dabei fokussierten die Teilnehmer der Arbeitsgruppe auf zwei größere Aspekte. Zum einen wurde die Etablierung einer Vertrauenskultur angeregt, wobei hier die Schwierigkeit besteht geeignete Kriterien zu etablieren und außerdem die Messung von Vertrauen eine Einigung auf Indikatoren voraussetzt. Zum anderen wurde die Bedeutung der Stärkung von Reflexionspotenzial in Bezug auf Überwachung(stechnologien) thematisiert. Konkret wurde überlegt Überwachung als Thema in Schulen auf den Lehrplan zu setzen, um einen aufgeklärteren Umgang mit diesem Phänomen zu befördern anstatt beispielsweise einfach zu behaupten, die jüngere Generation wäre nicht an Datenschutzfragen interessiert.

7.2 AG II: Überwachung in der Praxis: Technische Innovationen und deren Potentiale

Moderation: Matthias Wählisch, Freie Universität Berlin & Mark Palkow, daviko - Gesellschaft für digitale audiovisuelle Kommunikation mbH

Ausgangspunkt

Neue und zukünftige Technologien werden die Möglichkeiten, Räume, Daten und Menschen (automatisiert) zu überwachen, verändern. Der zunehmende Rückgriff und Gebrauch von Technik, um auf sicherheitsrelevante Herausforderungen zu reagieren, führt zur Frage, wie sich Überwachung aus technischer Perspektive betrachten und bewerten lässt und welche Empfehlungen sich für politische Entscheider daraus ableiten lassen. Dies beinhaltet auch eine Debatte darüber, ob das was technisch möglich ist, in jedem Fall angewendet werden oder ob hier in irgendeiner Art und Weise Beschränkungen vorliegen sollten.

Der Arbeitsgruppe wurde eingangs ein Auszug aus Dürrenmatts Roman ‚Die Physiker' präsentiert, der den folgenden Dreisatz beinhaltete:

1. Der Inhalt der [Technik] geht die [Techniker] an, die Auswirkung alle Menschen.
2. Was alle angeht, können nur alle lösen.
3. Jeder Versuch eines Einzelnen, für sich zu lösen, was alle angeht, muss scheitern.

(F. Dürrenmatt: „Die Physiker", 1962)

Die hierin geäußerte Sichtweise auf das Verhältnis zwischen Technik und Gesellschaft deutet darauf hin, dass der gesellschaftliche Umgang mit Technik nur als kollektiver Problemlösungs- und Gestaltungsprozess zu begreifen ist.

Inhaltliche Schwerpunkte

Die Arbeitsgruppe einigte sich darauf, den Fokus der Diskussion in erster Linie auf (automatisierte) Videoüberwachung zu legen und weniger auf Überwachungstechnologien wie RFID oder Biometrie. Zudem wurde eingangs eine Unterscheidung zwischen ‚sichtbaren' und ‚unsichtbaren' Technologien angeregt. Sichtbarkeit bezeichnet hierbei die direkte Nachvollziehbarkeit der Funktionsweise aus den materiellen Eigenschaften der Überwachungstechnologie (also z. B. wohin blickt die Kamera?), während sich das Unsichtbare auf Überwachungsformen, die im Verborgenen operieren bezog. An dieser Stelle wurde allerdings schnell klar, dass eine Trennung nur für manche Fälle sinnvoll erscheint, da etwa auch sichtbare Formen der Videoüberwachung intransparente Funktionen beinhalten können. Aus diesem Grunde wurde eine weitere Differenzierungsebene eingebracht, nämlich die zwischen Aufzeichnung, Speicherung und Auswertung. Diese drei Modi sollten schließlich mehr analytische Genauigkeit in der Diskussion ermöglichen.

Die Diskussion gliederte sich insgesamt in drei größere Bereiche – Funktionsweise und Potenziale von Überwachungstechnologien, soziale Auswirkungen und Möglichkeiten der Regulierung – auf die im Folgenden näher eingegangen werden soll.

Funktionsweise und Potenziale von Überwachungstechnologien

Hinsichtlich der Funktionsweise von Überwachungstechnologien wurde darauf aufmerksam gemacht, dass nicht nur die Erhebung von Daten durch einen datensammelnden Akteur problematisch ist, sondern vielmehr die Zusammenlegung und Kombination von mehreren Datensätzen, weil durch diese Verdichtung Muster erkennbar werden. Effektives Datenmanagement, etwa zum erfolgreichen Schutz der Privatsphäre, sollte sich demnach dieser Möglichkeiten bewusst werden und sowohl Qualität als auch Quantität der Erhebungsmethode und -technik daran anpassen.

Mit Blick auf die vielseitigen Potenziale von Überwachungstechnologien, wurde das klassische Argument der Reduzierung von Personalkosten angebracht, wobei auch kritisch reflektiert wurde, ob Technik wirklich gut geschultes Personal ersetzen könne. In dieser Perspektive wurde Technik lediglich als Hilfsmittel betrachtet in einer Weise, dass keine Entscheidungen an technische Systeme delegiert werden sollten, sondern versierte und gut ausgebildete Benutzer, die die Logik und Arbeitsweise des Überwachungssystems verstehen, unterstützt werden sollen.

Eine weitere Herausforderung bei der Entwicklung von Überwachungstechnologien wurde in der Unterschiedlichkeit von Laborsituation und Realität gesehen, weil die Testvoraussetzungen vor Einführung einer neuen Technologie oftmals unterkomplex sind, so dass Kriterien wie Validität, Reliabilität oder Objektivität nur selten gegeben sind. Dieser Aspekt wurde schließlich auch auf die oftmals zweifelhafte Konstruktion von Szenarien und Simulationen übertragen.

Soziale Auswirkungen von Technik und deren Akzeptanz

Dass das, was technisch möglich ist nicht automatisch auch sozial erwünscht ist, war der Einstiegsgedanke in die Diskussion über soziale Auswirkungen von Überwachungstechnologien. Somit wäre es der falsche Ansatz die ganze Palette der technischen Möglichkeiten im Bereich von Überwachung auszuschöpfen ohne dabei den konkreten Bedarf zu identifizieren und gezielt nach Lösungen Ausschau zu halten, die Abwägungen zwischen notwendigen Sicherheitsgewinnen und unnötigen Eingriffen in persönliche Freiheiten treffen.

In diesem Kontext wurde darauf hingewiesen, dass Unterschiede zwischen verschiedenen Anwendungsgebieten von Überwachung existieren, was sich jeweils auf die Tiefe des Eingriffs auswirken kann. So unterscheiden sich etwa die Überwachung öffentlicher Räume und die Überwachung des Arbeitsplatzes in mehrfacher Hinsicht, wenn letztere gezielt zu Verhaltens- und Leistungskontrollen herangezogen werden kann.

Hinsichtlich der Akzeptanz von Überwachung wurde zum einen der Nutzenaspekt thematisiert, wenn man zum Beispiel die Überwachung von Bahnhöfen oder Parkhäusern in der Nacht mit einer Steigerung des subjektiven Sicherheitsgefühls in Beziehung setzt. In dieser Sichtweise ist Überwachung eine Dienstleistung, die den individuellen Nutzen in den Fokus rückt. Zum anderen wurde die Bedeutung der symbolischen Ebene für die Herausbildung von Akzeptanz angesprochen. Wie es die öffentliche Debatte um den sogenannten ‚Nacktscanner' gezeigt habe, sei die Akzeptanz durch den negativ konnotierten Wortlaut stark eingeschränkt. Dies zeige sich auch an der gestiegenen Akzeptanz nach der Umbenennung in ‚Körperscanner'.

Somit stellte sich die Frage, auf welche Weise denn überhaupt gesellschaftlicher Konsens hinsichtlich der Entwicklung und Nutzung von Überwachungstechnologien hergestellt werden kann. Neben dem Verweis auf diverse *impact assessment*-Methoden wurde hier ein interdisziplinärer Entwicklungsprozess favorisiert, der eine Multistakeholder-Beteiligung ermöglicht und zudem das Zusammenspiel und die Zuordnung bestimmter Verantwortlichkeiten und Regulierungsoptionen bereits zu Beginn des Entwicklungsprozesses festlegt und mitdenkt.

Möglichkeiten der Regulierung

Dem Aspekt der Regulierung wurde innerhalb der Arbeitsgruppe gesonderte Aufmerksamkeit geschenkt. Hierbei wurde zum einen zwischen *ex ante*- und *ex post*-Regulierungsoptionen differenziert. Regulierung, die etwa bereits im Prozess der Technikentwicklung das Missbrauchspotenzial von Datenerhebungen berücksichtigt, entspricht dabei der *ex ante*-Strategie. Hierauf nehmen technische Gestaltungsprinzipien, wie beispielsweise *privacy by design*, Bezug. *Privacy by design* beschreibt dabei den Versuch den Schutz der Privatsphäre proaktiv im Entwicklungsprozess einer Technologie mit zu berücksichtigen, indem Informationen auf ein notwendiges Minimum abstrahiert werden. Das bedeutet, dass, wo es sich anbietet, Verschlüsselungstechniken und Kodierungen verwendet werden, um die Sammlung und Analyse von personenbezogenen Daten soweit wie möglich zu minimieren. *Ex Post*-Regulierung auf technischer Ebene entspricht dabei der Abstrahierung von Daten erst nach der Aufnahme (durch Filterung, Verpixelung etc.). Problematisch wurde an dieser Variante gesehen, dass ein Filter immer irgendwie überwunden bzw. deaktiviert werden kann, so dass ein Missbrauchsschutz auf technischer Seite immer irgendwie umgangen werden kann, was sich auf die subjektiven Einstellungen der Nutzer zur Technik auswirken könnte. Denn Vertrauen zu technischen Systemen kann wohl eher aufgebaut werden, wenn die Zweckentfremdung von Daten gar nicht erst möglich ist. Die Speicherung von Daten wurde dabei v. a. dann als problematisch erachtet, wenn es sich um personenbezogene Daten handelt. Die Vorgehensweise Daten prinzipiell nicht zu speichern und das analytische Ergebnis ausschließlich an das Erkenntnisinteresse anzupassen, um einen möglichst hohen Abstraktions- und Anonymisierungsgrad zu generieren, sollte folglich vorgezogen werden. Allerdings wurde an diesem Punkt angemerkt, dass Kunden häufig an maximaler Datenzugänglichkeit interessiert sind. Manche Unternehmen handhaben es deshalb so, dass man an die ungefilterten Aufnahmen z. B. nur über das Einverständnis des Betriebsrats gelangt. Hier wurde erneut deutlich, dass zwischen öffentlich-rechtlicher und privatwirtschaftlicher Regulierung zu unterscheiden ist.

Die Notwendigkeit und Ausgestaltung von Regulierungen könnte sich hierbei aus Kosten-Nutzen-Analysen ergeben, die auf einer Abwägung zwischen positiven und negativen Auswirkungen basieren. Sollte ein besonderer Mehrwert gegen eine vollständige Abstraktion und Anonymisierung von Daten sprechen, müsste man dies in Erwägung ziehen. Es stellt sich an dieser Stelle jedoch die Frage, wer diesen Mehrwert definiert und inwieweit die betroffenen Akteure in solch einen Entscheidungsprozess einbezogen werden können, gerade wenn es sich um privatwirtschaftliche Interessen handelt. In diesem Zusammenhang wurde Transparenz als Voraussetzung für das Instrument der Regulierung von Nutzerseite angesehen, da die Funktionsweise von technischen Überwachungssystemen aufgrund des hohen Grads an Komplexität für Laien nur schwer nachvollziehbar ist. In jedem Fall wurde ein Abstimmungsbedarf zwischen Wissenschaft und Wirtschaft als wichtig erachtet, um erstens die

Innovationsfähigkeit zu optimieren und zweitens um den jeweiligen Bedarf zielgerichtet zu verfolgen. Auch hierbei sollte allerdings klar sein, dass ein Sicherheitszugewinn durch Innovationen nur schwer messbar ist und dass der Bedarf nicht immer spezifiziert werden kann. Dennoch kann die Eindämmung von *dual use*-Problematiken nur auf diese Weise forciert werden. Hinsichtlich der rechtlichen Möglichkeiten der Regulierung (als weitere *ex post*-Option) wurde die Klärung von rechtlichen Grauzonen als wichtig erachtet. Regularien sollten hier möglichst genau an die ‚Realität' angepasst werden, damit sie sinnvoll nutzbar und durchsetzbar sind. Bei Nichteinhaltung dieser Regularien sollten Möglichkeiten der rechtlichen Sanktionierung herangezogen werden. Anstatt aber nur auf Sanktionen zu bauen wurde angeregt, Anreize für nutzerfreundliche, die Privatsphäre etc. schützende Technologien zu schaffen, was z. B. durch Siegel oder Zertifikate erfolgen könnte. Eine Zertifizierungsstelle könnte auch sichtbar machen, wofür Technik genutzt werden kann, weshalb Zertifizierung förderlich für die Akzeptanz sein könne. Die Mehrausgaben für Siegel und Zertifikate könnten sich somit am Ende auch marktwirtschaftlich lohnen.

Thesen, Handlungsempfehlungen und Botschaften

Die Thesen, Empfehlungen und Botschaften der Arbeitsgruppe wurden wie folgt zusammengefasst:

1. Daten-Management

Es fehlen für den Bürger (weiterhin) Prüfstellen für das Daten-Management. Hier ist ein höheres Maß an Transparenz und Informationsarbeit notwendig.

2. Akzeptanz

Die Akzeptanz ist im staatlichen, unternehmerischen und privaten Bereich unterschiedlich gelagert.

3. Zusatznutzen/Mehrwert

Der Mehrwert sollte vollständig ausgeleuchtet werden, um besser zu regulieren und die Akzeptanz zu erhöhen.

4. Regulierung

Wir brauchen keine Sanktionen, sondern Regulierungen. Die bisherigen Regulierungen sind unzureichend, da noch zu viele Schlupflöcher existieren. Die Regulierungen sollten so konkret wie möglich und so abstrakt wie nötig – ergo: praxisnah – gestaltet werden.

7.3 AG III: Politischer Wille und gesetzliche Grenzen im Umgang mit Überwachung

Moderation: Dr. Johannes Eichenhofer, Universität Bielefeld & Nils Leopold, Büro Konstantin von Notz (MdB)

Ausgangspunkt

Überwachung ist zweifelsohne kein neues Phänomen, wie sich beispielhaft am bekannten Werk ‚Überwachen und Strafen' von Michel Foucault aus dem Jahr 1975 ablesen lässt. Allerdings treten in der heutigen Debatte vermehrt die technischen Möglichkeiten von Überwachung in den Vordergrund. Ausgangspunkt der AG-Arbeit war damit die Frage, wo Überwachung und Überwachungstechnologien Grenzen durch Politik und Recht gesetzt sind oder gesetzt sein sollten.

Goldgräberstimmung

Diskutiert wurden einleitend Fragen nach den Kontrollmöglichkeiten des Bundestages und den Handlungsmotiven der Regierungsparteien im Kontext von Überwachung. Aus politischer Sicht wurde deutlich, dass eine regelrechte „Goldgräberstimmung" in den entsprechenden Kreisen des Bundestages und der involvierten Lobbyvertreter herrscht. Große Unternehmen stehen im regen Austausch mit Vertretern der Politik, um ihre technischen Innovationen vorzustellen, die auf ein durchaus positives Echo zumindest der großen Parteien stoßen würden. Dies liegt u.a. daran, dass für die Regierungsparteien ein großes Interesse besteht, Sicherheitsgewährleistung sichtbar zu machen, um die Akzeptanz der Bevölkerung nicht zu verlieren. In Bezug auf die Kontrollfunktion des Bundestages ist dabei insbesondere der Aspekt staatlicher Aufrüstung im Überwachungsbereich von Interesse. Sicherheitsbehörden benutzen heute Technologien (und generieren mit diesen Daten), von denen man bis vor kurzem noch gar nicht wusste, dass sie in dieser Form existieren. Den Bundestag als Gesetzgeber stellt dies vor das Problem, exekutive Arbeit kontrollieren zu können.

Überwachung zwischen Freiheit und Sicherheit

Anhand mehrerer Beispiele aus internationaler Erfahrung (z. B. Automatisierte Unfallmeldung in entsprechend ausgestatteten Fahrzeugen in Schweden; Nachvollziehbarkeit von Standorten von Mietwagen durch Behörden in Japan) wurde zunächst die Frage diskutiert, wann überhaupt Überwachung beginnt. Es wurde deutlich, dass Überwachung in unterschiedlichen Formen vorherrscht und in diesen unterschiedlich wahrnehmbar und diskutiert ist. Während Überwachung im öffentlichen Raum noch weitestgehend „sichtbar" erfolgt, ist datenbezogene Überwachung durch Tracking, mobile Kommunikation und Internettechnologien kaum mehr erfassbar. Hierbei tritt das Problem in den Vordergrund, dass politische Entscheider nur sehr bedingt in der Lage sind, Möglichkeiten (und damit auch Grenzen) dieser Technologie abzuschätzen. Damit muss sich Politik die Frage stellen, wie mit potenziellen Nebenfolgen umgegangen werden kann: Wie lassen sich neue technische Entwicklungen nachverfolgen, wie lässt sich die Verwendung von Technologien in anderen Kontexten / für andere Zwecke absehen und inwieweit ist Politik in der Lage zu erkennen, welche Folgen in der heutigen Rechtsprechung hinsichtlich der technologischen Entwicklung in fünf Jahren denkbar sind?

Hinsichtlich der Rechtsetzung lässt sich festhalten, dass diese bislang reaktiv erfolgt und in der Regel erst Jahre später auf neue Technologien reagiert. Hier sollte stärker über antizipierende Rechtssetzung

nachgedacht werden, um die demokratische Kontrolle und Legitimation von technischen Maßnahmen der Überwachung zu sichern.

Wertvorstellungen zu Überwachung

Die Technikentwicklung ist in der Regel schneller als ein gesamtgesellschaftlicher Meinungsbildungsprozess zur Sinnhaftigkeit einerseits und dem Gefährdungspotential neuer Technologien andererseits. Ein politisch initiierter öffentlicher Diskurs erfolgt in der Regel erst, wenn neue Technologien mit hohem Potenzial zum Missbrauch (z. B. für Überwachung) bereits in der Gesellschaft verankert sind. Offen bleibt hier die Frage, wie man mit unterschiedlichen Wertvorstellungen im internationalen Kontext umgeht. Während sich spezifische Technologien weltweit durchsetzen, reagieren unterschiedliche Akteure zumeist mit national geprägten Wertvorstellungen und interpretieren vor dem Hintergrund dieser die Vor- und Nachteile technischer Innovationen unterschiedlich.

Vorratsdatenspeicherung und der Umgang mit Unsicherheit

Im Kontext des Themas Vorratsdatenspeicherung tritt der Konflikt zwischen Sicherheit und möglicher Einschränkung von Freiheit besonders zu Tage. Einerseits gibt es Gründe, die für den Einsatz sprechen (Terrorismusbekämpfung), andererseits führt die Nutzung dieser Daten zu anderen Zwecken immer mehr zu einer Gewohnheit der Überwachung. Auch an diesem Beispiel zeigt sich, dass ein steter Diskurs darüber, welche Gefährdungen akzeptierbar erscheinen und welche nicht, dauerhaft und nicht abschließend geführt werden sollte. Die Akzeptanz von Unsicherheit als Bestandteil des Lebens bleibt jedoch politisch äußert schwierig zu transportieren. Nichtsdestotrotz liegt in einem anvisierten gesellschaftlichen Wandel, der zu einer rationaleren Einschätzung führt (z. B. Gefährdung im Alltag vs. Gefährdung durch Terrorismus) ein wichtiges Ziel politischen Handelns. Auch in einem gesellschaftlichen Verständnis des Umgangs mit Restrisiken und Unsicherheiten bleibt Sicherheit ein menschliches Grundbedürfnis. Die Frage jedoch ist, wie dieses mit begrenzten Ressourcen bedient wird. Die Diskussion zeigt, dass es eine stete Auseinandersetzung über die Prioritäten in der Sicherheitsdiskussion geben muss: Wie viel Geld wird z. B. in Verkehrssicherheit investiert, wie viel in Überwachung?

Geheimdienste und Polizei

Grundsätzlich sind Geheimdienste voneinander zu unterscheiden. Während Polizeiarbeit dokumentiert und nachvollziehbar erfolgt, kann eine Kontrolle der Geheimdienstarbeit durch das Parlament nur auf Basis von Selbstauskünften erfolgen. Wenn Geheimdienste nicht offenlegen, was für neue Technologien sie benutzen, erfahren Parlamentarier dies auch nicht.

In der Geheimdienstarbeit scheint sich ein neuer Ethos des „was technisch möglich ist, machen wir“ zu etablieren. Bedenken gegenüber dem Einsatz neuer Technologien stehen hinter operativen Zielen der Geheimdienstarbeit zurück. Informationsgenerierung geht hier vor ethischen Bedenken.

Empfehlungen der Arbeitsgruppe

1. Recht muss im Sinne einer Regulierung grundlegend und ständig weiterentwickelt werden. Begleitende Maßnahmen zur effizienten Durchsetzung müssen entwickelt werden (z. B. technisch und organisatorisch gestützte Lösungen)

- Technik darf sich nicht unreflektiert weiterentwickeln
- Die Verantwortung in der Überwachungsdebatte darf nicht einfach von Politik auf Technik übertragen werden
- Die Grenzen der Regulierung müssen benannt werden (Was kann der Gesetzgeber regulatorisch noch erreichen?)
- Recht ist gesetzte Norm der Vergangenheit

2. Politik kann Rahmenbedingungen hinsichtlich der Information (Mündigkeit der Bürger) schaffen, um eine gesamtgesellschaftliche (Werte-)Diskussion zu unterstützen.

- Überwachung als Lösung zwischen Freiheit und Sicherheit muss Gegenstand fortwährender Diskussionen sein
- Wie sicher wollen wir leben und wie viel Unsicherheit sind wir bereit auszuhalten?

3. Die Differenzierungs- und Diskursfähigkeit zur öffentlichen Sicherheit in Deutschland muss als besonderes Merkmal (auch international) in den Vordergrund gestellt werden.

- Internationalisierungstendenzen sollten zu einer selbstbewussten Gegenposition führen, statt in einem Wettbewerb zu enden
- Es muss eine Balance zwischen nationalen (Kameraüberwachung in Deutschland) und internationalen Kontexten (Onlineüberwachung internationaler Dimension) gefunden werden
- Die historisch gewachsene Kritikfähigkeit in der deutschen Diskussion muss (politisch und zivilgesellschaftlich) erhalten bleiben und gefördert werden. Sie sollte als positives Merkmal herausgestellt und wenn nötig zur Abgrenzung genutzt werden.