

**Universität
Augsburg**



**Philosophisch-Sozialwissenschaftliche Fakultät
Lehrstuhl für Politik/ Politische Theorie
Prof. Dr. Marcus Llanque**

Technische Überwachung

Die freiheitliche demokratische Gesellschaft am Scheideweg

Bachelorarbeit

Erstprüfer: Prof. Dr. Marcus Llanque

Zweitprüfer: Prof. Dr. Christoph Lau

Abgabe:
17.08.2010

vorgelegt von:
Kleber Paul
1020902
Stettenstraße 32
86150 Augsburg

Studiengang:
BA Sozialwissenschaften
6. Fachsemester

Sommersemester 2010

**„we shape our tools,
and thereafter our tools shape us“**

Marshall McLuhan

Für Martina.

Und für meine Familie und Freunde. Danke für´s warten.

Inhaltsverzeichnis

1. Wissen ist Macht.....	5
2. Technische Überwachung.....	8
2.1 Kommunikationsüberwachung am Beispiel der „Vorratsdatenspeicherung“:.....	9
• <i>Definition</i>	9
• <i>Hintergrund</i>	9
• <i>Gesetzliche und politisch-rhetorische Implementation</i>	10
• <i>Erhobene Daten</i>	12
• <i>Verkehrsdatenanalyse und daraus entwickeltes Wissen</i>	14
• <i>Entzugsmöglichkeiten</i>	17
• <i>Kritik erster Ordnung</i>	18
2.2 Biometrie: Der neue „ePass“ und der „ePA“	20
• <i>Definition</i>	20
• <i>Hintergrund und Geschichte</i>	20
• <i>Gesetzliche und politisch-rhetorische Implementation</i>	21
• <i>Erhobene Daten</i>	24
• <i>Kritik erster Ordnung</i>	26
• <i>Entzugsmöglichkeiten</i>	33
2.3 Recht am eigenen Bild: „Nacktscanner“	35
• <i>Definition</i>	35
• <i>Gesetzliche und politisch-rhetorische Implementation</i>	35
• <i>Erhobene Daten</i>	36
• <i>Entzugsmöglichkeiten</i>	37
• <i>Kritik erster Ordnung</i>	37
2.4 Überwachung durch nicht-staatliche Akteure am Beispiel „Kundenscoring“	37
• <i>Definition</i>	38
• <i>Gesetzliche und politisch-rhetorische Implementation</i>	39
• <i>Erhobene Daten</i>	39
• <i>Kritik erster Ordnung</i>	40
3. Die fragmentierte Datenmacht.....	41
3.1 Daten.....	41
• <i>Begriffsdefinition: Daten</i>	41
• <i>Daten und ihr Fortpflanzungsmechanismus</i>	42

3.2 Kontrollverlust der Kontrolle.....	43
• <i>Elektronische Datensicherheit im Allgemeinen und im staatlichen Raum</i>	43
• <i>„Klassische“ Datenverluste in der näheren Vergangenheit</i>	45
• <i>Datenverlust am Beispiel der Monitorabstrahlung</i>	45
• <i>Daten-Akteure</i>	46
• <i>Langzeitwirkung von Daten</i>	48
• <i>Zwischenfazit</i>	49
4. Gesellschaft unter Kontrolle?.....	50
4.1 Auswirkungen der Überwachung auf den Einzelnen.....	50
• <i>Persönlichkeitsentwicklung</i>	50
• <i>Die Rechte des Einzelnen</i>	52
• <i>Reaktion des Einzelnen am Beispiel von „Promis“</i>	53
4.2 Auswirkungen der Überwachung auf die Gesellschaft	54
• <i>Die freiheitliche demokratische Grundordnung</i>	54
• <i>Gefahren für die Gesellschaft</i>	55
5. Gesellschaft am Scheideweg.....	58
Abkürzungsverzeichnis	60
Literaturverzeichnis.....	61

1. Wissen ist Macht

Seit dem 11. September 2001 wissen wir, dass Nichts und Niemand sicher ist. Unser beschauliches Leben könnte jederzeit zu Ende sein. So genannte „Schläfer“ leben unerkannt unter uns und warten darauf, irgendwann, wenn niemand damit rechnet, erbarmungslos zuzuschlagen und Tausende in den Tod zu reißen.

Doch „wissen“ wir das wirklich?

Seit der Einführung des Konstruktivismus „wissen“ wir, dass die Realität in der wir Leben konstruiert wird. Und zwar von uns allen, aber nicht von allen in gleichem Maße.

Je nachdem welche Interpretationshoheit einem Individuum oder einer Institution zugeschrieben wird, ist es dieser leichter oder schwieriger neues Wissen zu generieren und in der gesellschaftlichen Realität zu verankern. Wissen beschreibt hier also sowohl die Agglomeration von „Fakten“, als auch deren Interpretation – zwei Dinge die jedoch niemals voneinander getrennt werden können, da es reine Fakten nach dem Konstruktivismus nicht gibt, bzw. diese nicht vom Menschen in Reinform wahrgenommen werden können.

Wer Macht hat, kann Wissen generieren. Aber: Wissen ist Macht.

Oder wie Michel Foucault es ausdrückt:

„[Es] ist wohl anzunehmen, dass die Macht Wissen hervorbringt [...]; dass Macht und Wissen einander unmittelbar einschließen; dass es keine Machtbeziehung gibt, ohne dass sich ein entsprechendes Wissensfeld konstituiert, und kein Wissen, das nicht gleichzeitig Machtbeziehungen voraussetzt und konstituiert. Diese Macht/Wissen-Beziehungen sind darum nicht von einem Erkenntnissubjekt aus zu analysieren, das

gegenüber dem Machtsystem frei und unfrei ist. Vielmehr ist in Betracht zu ziehen, dass das erkennende Subjekt, das zu erkennende Objekt und die Erkenntnisweisen jeweils Effekte jener fundamentalen Macht/Wissen-Komplexe und ihrer historischen Transformationen bilden.¹

Zu den bedeutendsten Wissensproduzenten gehört die Wissenschaft. Auch wenn ihr gelegentlich (zu recht) vorgeworfen wird, etwa durch Fördergelder korrumpiert zu sein, so gelten wissenschaftliche Veröffentlichungen zu den mächtigsten Werkzeugen, welche in einen gesellschaftlichen Diskurs eingebracht werden können.

Kommen wir zurück zum Elften September. Dass sich die Welt seit dem verändert hat ist unumstritten. Vor allem hat sich jedoch die gesellschaftliche Wahrnehmung bezüglich Freiheitsrechten und Überwachung verändert.

In den Jahren danach wurden viele neue Gesetze implementiert, welche vor allem neue Überwachungssysteme einführten.

Prägend waren in dieser Zeit vor allem Politiker, die mit immer noch farbenfroheren „Horrorszenarien“ die Realität der Bürger prägten.² Gleichzeitig hielt sich die Wissenschaft erstaunlicherweise weitestgehend zurück.

So argumentierten Überwachungsbefürworter und -gegner häufig „freihändig“, ein gesellschaftliches Gesamtkonzept, nach welchem sich die aktuelle Politik auszurichten habe, ist zur Zeit nicht erkennbar.

1 Foucault, Michel (1976): Überwachen und Strafen. Die Geburt des Gefängnisses, S. 39f.

2 So warnte etwa Innenminister Wolfgang Schäuble bei SpiegelOnline vor Terroranschlägen mit „Schmutzigen Bomben“: Spiegel Online (2006): Terror-Gefahr. Schäuble erwartet Anschlag mit schmutziger Bombe

Diese Arbeit bemüht sich daher darum eine Grundlage für eine umfassende Diskussionen zu schaffen. Der Fokus liegt dabei darauf, wissenschaftliche Fakten zu aufzubereiten, so dass diese zumindest in den sozialwissenschaftlichen Diskurs einfließen können.

Hierfür werden im ersten Teil technische Überwachungssysteme betrachtet, sowohl hinsichtlich der erhobenen Daten, als auch hinsichtlich der Argumentation, welche zu ihrer Einführung führten. Im anschließenden Teil werden die Eigenheiten von elektronischen Daten genauer untersucht. Nachfolgend werden die Auswirkungen der vorhergehend erzielten Erkenntnisse auf die Gesellschaft umrissen.

Primär werden dabei technische und soziologische Fakten durch Primärquellen ausgewiesen, die politisch-rhetorische Implementationsgeschichte durch populärwissenschaftliche Quellen wie Zeitungsberichte belegt.

2. Technische Überwachung

Um die Auswirkungen von Überwachung auf den Bürger betrachten zu können, ist es nötig herauszufinden, in wieweit und mit welchen Mitteln diese stattfindet.

Hierfür werden im folgenden Kapitel technische Mittel, welche

a) bereits im Rahmen gesetzlicher Vorschriften angewendet werden (dürfen bzw. müssen) oder durch bestehende Gesetzesinitiativen zur Anwendung gebracht werden sollen, oder durch internationale Verträge zu implementieren sind, und

b) einen größeren Bevölkerungsteil betreffen, so dass diese als gesamtgesellschaftlich relevant zu betrachten sind,

soweit beschrieben, dass ihre Auswirkungen anhand der durch diese aggregierten Datensammlungen und Einzeldaten, sowie deren Aussagekraft und Wirkungszusammenhänge in den Diskurs eingebracht werden können. Hierbei werden auch relevante rhetorische, politische und verfahrenstechnische Implementationsstrategien angemerkt.

Die Arbeit konzentriert sich hierbei auf Deutschland, jedoch wird der Blick auch auf das (vornehmlich europäische) Ausland erweitert da die Betrachtung einer (globalisierten) Gesellschaft als rein national-staatliches Konstrukt als anachronistisch zu bezeichnen ist,³ und auch Daten keine Ländergrenzen kennen⁴.

In diesem Zusammenhang ist es wichtig, sich stets die Grenzen der Geltungsbereiche verschiedener Datenschutz-Standards im Hinterkopf zu behalten.

3 Vgl. hierzu: Cappel, Christian(2006): Anachronismus einer „Drittwirkung“ - Das kognitivistische Konzept Karl-Heinz Ladeurs und die Matrix Gunther Teubners im grundrechtstheoretischen Spannungsfeld, S.41- 53

Dieses Werk beleuchtet des weiteren einige Aspekte der in dieser Arbeit verhandelten Thematik von einer gänzlich anderen Sichtweise und ist dem Leser als Zweitlektüre nahe gelegt.

4 Vgl. Mitteilung des Referatsleiters beim Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein: Hill, Werner(1998): Erfassen, löschen und vernichten – Der Mensch in der Datei, S.49-51

2.1 Kommunikationsüberwachung am Beispiel der „Vorratsdatenspeicherung“:

- **Definition**

Als „Vorratsdatenspeicherung“ bezeichnet man das Mittel der *anlasslosen* Speicherung umfangreicher Daten *sämtlicher* Nutzer elektronischer Kommunikationsdienste. Hierfür werden von Seiten der Netzbetreiber Datenbanken aufgebaut, die (staatlichen) „Bedarfsträgern“ unter bestimmten Voraussetzungen offen stehen.

- **Hintergrund**

Die so genannte „Vorratsdatenspeicherung“ (im Nachfolgenden VDS abgekürzt) gleich zu Beginn dieser Betrachtung zu untersuchen mag auf den ersten Blick ungeschickt erscheinen, da das Bundesverfassungsgericht erst kürzlich die Vorratsdatenspeicherung in Deutschland für verfassungswidrig und die entsprechenden Vorschriften für nichtig erklärt hat.

Jedoch wurde zum ersten die VDS vom höchsten deutschen Gericht nicht per se als Instrument der Strafverfolgung und Gefahrenabwehr verworfen, sondern nur in ihrer konkreten Ausgestaltung.⁵ Das Gesetz sehe „nur“ keine konkreten Maßnahmen zur Datensicherheit vor und die Hürden für den Abruf dieser Daten seien zu niedrig. Dem deutschen Bundestag steht es also jederzeit frei, die gesetzlichen Rahmenbedingungen für einen weiteren Anlauf zu schaffen. Dies wird nach Angaben von Bundesinnenminister Thomas de Maizière von der Bundesregierung auch geplant.⁶

Zum zweiten fußt das Gesetz auf einer EU-Richtlinie, welche somit für 450 Millionen EU-Bürger Gültigkeit besitzt. Dies hat nicht nur

5 Bundesverfassungsgericht (2010): 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

6 Schönherr, Maximilian (2010): „Herr de Maizière und sein Radiergummi -Bundesinnenminister will Grundlagen der Internetpolitik neu ordnen“

indirekte Auswirkungen im Rahmen der Betrachtung einer globalisierten Gesellschaft, es bedeutet auch dass Kommunikation über Ländergrenzen hinweg weiterhin protokolliert wird. Hierfür ist es nicht nötig, dass ein Teilnehmer sich in einem entsprechenden Staat aufhält, es reicht dass eine Vermittlungsstelle der Kommunikation (Proxy, Host, etc.) dem Geltungsbereich dieses oder eines ähnlichen Instrumentes unterliegt.

Drittens ist Kommunikation konstituierendes Element für die Kultur einer Gesellschaft, ja für die Gesellschaft selbst.⁷ Ein Eingriff in die Kommunikation ist daher von grundlegender Bedeutung.

• Gesetzliche und politisch-rhetorische Implementation

Die VDS wurde in Deutschland mit dem „*Gesetz zur Neuregelung der Telekommunikations-überwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*“⁸ eingeführt. Dieses Gesetz fußt, wie der Name verrät, auf der EU-Richtlinie zum „*anlassunabhängige[n] und nicht zweckbezogene[n] Sammeln von personenbezogenen Daten zur späteren Verwendung*“⁹. Diese Richtlinie ist für die Mitgliedsländer bindend und muss in nationales Recht übergehen, jedoch steht es diesen frei die Speicherpflicht zwischen sechs Monaten und zwei Jahren festzulegen.

Da das Mittel klar der Sphäre der Gefahrenabwehr zuzuordnen ist, und damit ausdrücklich nicht in den Kernbereich des Staatenbundes fällt, berief sich die EU auf ihre „Binnenmarktkompetenz“ (Artikel 95 EGV) und argumentiert, so gleichartige Marktchancen in den Mitgliedsländern zu etablieren.

7 Vgl. McLuhan, Marshall (1992): *The Global Village: Transformations in World Life and Media in the Twenty-First-Century*

8 Europäisches Parlament (2006): *Richtlinie 2006/24/EG Des Europäischen Parlaments und des Rates*

9 Ebd. L 105/54

Gleichzeitig bezog man sich jedoch auf die am 23. November 2001 vom Europarat beschlossene „Convention on Cybercrime“, in welcher man zu der Überzeugung gekommen sei, *„dass „zur wirksamen Bekämpfung der Computerkriminalität eine verstärkte, zügige und gut funktionierende internationale Zusammenarbeit in Strafsachen nötig ist“¹⁰.*

Dieser argumentative Umweg, bzw. das Ausweichen auf eher sachfremde Institutionen und Kompetenzen mag außergewöhnlich erscheinen, hat auf EU-Ebene jedoch Tradition.¹¹

Erstaunlicher mutet es an, wenn man bedenkt, dass schon vor der Schaffung der EU-Richtlinie zweimal versucht wurde die VDS in Deutschland per Gesetz zu legitimieren:

2002 in Niedersachsen und 2005 als gesamtdeutscher Gesetzesvorstoß. Dieser Gesetzesentwurf passierte zwar den Bundesrat, im Bundestag fiel er jedoch wegen verfassungsrechtlicher Bedenken durch.¹²

Dass das Gesetz bei seiner Neuauflage die benötigten Stimmen erhielt, obwohl die verfassungsrechtlichen Bedenken nicht ausgeräumt wurden, ist eines eher spektakulären Denkansatzes geschuldet, welcher dem Beschluss als offizielle Erklärung beigefügt wurde:

„Eine Zustimmung ist auch deshalb vertretbar, weil davon auszugehen ist, dass in absehbarer Zeit eine Entscheidung des Bundesverfassungsgerichts möglicherweise verfassungswidrige Bestandteile für unwirksam erklären wird.“¹³

10 Europarat (2001): Übereinkommen über Computerkriminalität

11 So wurde zum Beispiel 2005 versucht über einen Beschluss des EU-Fischerei- und Landwirtschaftsrates Softwarepatente in der EU zu legalisieren.

12 Deutscher Bundestag (2006): Plenarprotokoll 15/157, S. 14-33

13 Erklärung von 26 SPD-Fraktionsmitgliedern nach §31 der Geschäftsordnung des Deutschen

Die Verantwortung wurde ausgelagert.

Auf EU-Ebene wird derzeit die Ausweitung der VDS auf Suchmaschinen vorbereitet. In einer "written declaration" (deutsch meistens „gemeinsamer Standpunkt“) sprach sich die erforderliche Mehrheit der EU-Parlamentarier im Sommer 2010 dafür aus, die Richtlinie 2006/24/EG umzusetzen und deren Zuständigkeitsbereich zu erweitern.¹⁴

• Erhobene Daten

Die bei der „Vorratsdatenspeicherung“ erhobenen Daten *erfolgreicher und missglückter* elektronischer Kommunikation lassen sich in drei Gruppen unterscheiden:

Primär werden so genannte „Verkehrsdaten“ erhoben. Dieser Block umfasst die Rufnummer des Anrufers sowie des Angerufenen (Telephon), die IP (Eine Art „Rufnummer des Internet-Anschlusses“) des oder der benutzten Computer sowie etwaiger Server, auf die zugegriffen wird (Internet). Benutzt ein Teilnehmer ein Mobiltelefon werden zudem die so genannten IMAP- und IMSI-Nummern erhoben. Hierbei handelt es sich jeweils um eine eindeutige Identifikationsnummer des Handys bzw. der Sim-Karte.

Anders ausgedrückt wird erhoben (1) *wer* (2) *mit wem* (3) *wie lange* (4) *mit welchen Mittel* kommuniziert.

Die nächste Datengruppe umfasst die Begleitumstände der Kommunikation. Hierbei sind vor allem die Informationen über den Aufenthaltsort, also das (5) „*wo*“, herauszuheben:

Bei Handys wird z.B. der Standort des Anrufbeginns und der Aufenthaltsort zum Ende des Anrufes festgehalten. Diese Erfassung

Bundestages : Deutscher Bundestag (2007): Plenarprotokoll 16/124, Anhang 4, S.90
14 Motti, Tiziano/ Záborská, Anna (2010): Schriftliche Erklärung zur Schaffung eines europäischen Frühwarnsystems gegen Pädophilie und sexuelle Belästigung

der „Geodaten“ bezieht sich jedoch nicht nur auf das herkömmliche „Telefonieren“, sondern auf jede Art der mobilen Datennutzung wie Mail-Abruf via Mobiltelefon, SMS-Empfang und Versendung, Surfen via SMTP/WAP, etc.

Festgehalten wird der Standort des Benutzers durch die Zuordnung der „Funkzelle“, also die Information, welchem Funkmast, bzw. welchen Funkmasten das Gerät zum jeweiligen Zeitpunkt zugeordnet wurde.¹⁵ Die Genauigkeit der Standortbestimmung schwankt hierbei zwischen einigen Kilometern (etwa in einigen Regionen in Brandenburg) und wenigen Metern (zum Beispiel in Großstädten), kann jedoch durch „Time-Slot“-Interpretation¹⁶ noch deutlich genauer angelegt werden.

Bei anonymen Sim-Karten (wie sie im europäischen Ausland erworben werden können) wird zusätzlich der Ort der Erst-Aktivierung aufgezeichnet, um zumindest grobe Rückschlüsse auf den Besitzer ziehen zu können.

Der dritte Datentyp umfasst die Bestandsdaten, also die Daten über die Identität des Benutzers. (Auf wen ist das Telefon/der Internet-Anschluss/das Handy zugelassen; Wer bezahlt die Rechnung; Wo wohnt die Person, Informationen über das Zahlungsverhalten etc.)

¹⁵ Das Mobiltelefon-Netz ist so aufgebaut wurde, dass das Telefon während eines Gespräches den Standort wechseln kann. Das Gerät hält daher nicht nur Kommunikation mit dem Funkmast aufrecht, welchem es gerade zugeordnet ist, sondern auch mit den Nachbartürmen. Bei einem Standortwechsel wird es von einem Masten zum anderen weitergereicht.. (Dieses Weiterreichen der Zuständigkeit bezeichnet man als „Handover“). Durch die Kenntnis des Abstandes des Gerätes zu mehreren Funkmasten lässt sich der Standort (geometrisch) errechnen.

¹⁶ Teil der Kommunikationslogik des Mobiltelefonnetzes ist es, bestimmte Datenpakete in genau definierten Zeitintervallen abzusetzen. Diese Intervalle befinden sich im Bereich weniger Millisekunden. Durch die Kenntnis über die spezifische Laufweite - die Funkwellen einer bestimmten Frequenz nun einmal haben - und dem Antwortverhalten des Mobiltelefons, lässt sich so der Abstand in vielen Fällen bis auf wenige Zentimeter exakt bestimmen.

Bei weitergehendem Interesse bezüglich des Aufbaus und der Funktionsweise von GSM-Netzwerken empfehle ich: Pritlove, Tim(2007): GSM Hacking - Aufbau, Funktionsweise und Sicherheitsmängel von GSM-Netzwerken

Verkehrsdaten und Begleitumstände werden dabei jeweils mit den Bestandsdaten verknüpft, um eine Zuordnung in beide Richtungen zu ermöglichen.

• Verkehrsdatenanalyse und daraus entwickeltes Wissen

Das Instrument der Verkehrsdatenanalyse kommt ursprünglich aus dem militärischen bzw. geheimdienstlichen Sektor. Dennoch hat es auf Umwegen, und dies wird dem Leser wahrscheinlich unbekannt sein, Einzug in unsere Alltagssprache gehalten: Im geflügelten Wort der „Funkstille“.

Als zum Ende des ersten Weltkrieges die Verschlüsselung Einzug in den Funkverkehr hielt, und somit die Kosten für ein aktives Abhören des Feindes exponential stiegen, fanden Techniker verschiedener Nationen schnell heraus, dass es in den meisten Fällen nicht nötig ist, den Inhalt einer Kommunikationshandlung zu kennen - das pure Wissen über deren Existenz ist häufig schon aussagekräftig genug.

Wiederkehrende Kommunikation erzeugt Muster. So lässt sich schnell herausfinden, wer Entscheidungen trifft, an wen diese weitergeleitet werden, und wer Befehle empfängt.

Ohne zu wissen, welche Befehle übermittelt werden, ist schon auf den ersten Blick ersichtlich, welche Hierarchieebene ein Kommunikationsteilnehmer (beim Militär) zuzuordnen ist, und somit auch, wessen Kommunikation es ggf. Wert ist, entschlüsselt zu werden. Daher halten militärische Organisationen und Gruppierungen in spezifischen Situationen Funkstille um etwaigen Gegnern keine Hinweise auf bevorstehende Handlungen zu geben¹⁷ bzw. betreiben Scheinkommunikation um die spezifische Wichtigkeit verschiedener Kommunikationsteilnehmer zu verschleiern.

¹⁷ Jedoch kann auch die Funkstille als Information interpretiert werden, etwa wenn diese kurz nachdem auftritt, nach dem eine hohe Hierarchieebene in die Kommunikation eingegriffen hat.

Für die Generation, welche den „Kalten Krieg“ noch aktiv miterlebte, sei an dieser Stelle erwähnt, dass die Verkehrsdatenanalyse (nicht die Funkstille) fast den dritten Weltkrieg ausgelöst hätte - darin sind sich Militärgeschichtler beider Seiten mittlerweile einig. Auf negativen Folgen etwaiger Fehlinterpretation von Daten werde ich jedoch zu späterer Stelle noch einmal genauer eingehen.

Im vorliegenden Fall der Verkehrsdatenanalyse im Bereich der elektronischen Kommunikation der Bürger verhält es sich ähnlich wie beim Militär: Die alltägliche Kommunikation erzeugt „lesbare“ Muster, die erhebliche Einblicke in das Leben des Einzelnen selbst dann zulassen, wenn die Inhalte der Kommunikation verborgen bleiben:

Ruft ein Kommunikationsteilnehmer von einem Mobiltelefon aus, welches - durch die Bestandsdaten ersichtlich - auf eine unverheiratete weibliche Person Ende Zwanzig zugelassen ist, kurz nach einander ihren Frauenarzt, dann die katholische Fürsorge und schließlich einen Arzt, welcher auf Abtreibungen spezialisiert ist, an, so kann man die Lebensumstände der jungen Dame erahnen, ohne dass wir die genauen Gesprächsinhalte kennen müssen.

Zieht man hierzu noch die Internetaktivitäten, etwa ein häufiger Besuch auf einem Webserver einer Dating-Agentur, zusammen mit Online-Buchungen verschiedener Hotels und Restaurants hinzu, wird das Bild klarer.

Durch die Funkzellenanalyse wird sogar ersichtlich, mit wem sich unser fiktives Überwachungsoffer trifft. Selbst wenn die Beiden nie miteinander über ihre Handys oder ihre Festnetzanschlüsse miteinander kommuniziert haben, ist die bloße Tatsache, dass die Mobiltelefone unserer Probanden zu den bereits ermittelten Terminen teilweise in der selben Funkzelle SMS-Nachrichten empfangen oder

gesendet haben, ein stichhaltiger Hinweis.¹⁸ Eine Verkehrsdatenabfrage der zweiten Person verfestigt die vorliegenden Informationen.

Auch das Leben von Personen welches nicht, wie in diesem ausdrücklich plastischen Beispiel strukturiert ist, wird durch den Einsatz geeigneter Software maschinell lesbar. Die Strukturen von Freunden und Bekannten, das Verhältnis zu den Eltern – all das lässt sich mit einem einzigen Knopfdruck statistisch auswerten - allein durch die Information wer mit wem, wie oft, wann und auf welchem Weg, regelmäßig oder unregelmäßig kommuniziert und wo sich diese Personen dabei befinden. Kommunikation erzeugt Muster, welche Rückschlüsse auf die Art und Qualität von Beziehungen zulassen.

All diese Informationen können von geeigneter Software, welche auf dem freien Markt erhältlich ist, jedoch auch von Polizei und Geheimdiensten eingesetzt wird, automatisiert ausgewertet werden. Hierbei werden neben den Kommunikationsmustern auch (realweltliche) Bewegungsmuster erstellt – ausgehend von den Orten, an denen ein Mobiltelefon aktiven Kontakt zum Funknetz hatte – welche in einem Gutachten für das Bundesverfassungsgericht als "*nahezu lückenlose räumliche Überwachung*" beschrieben wird.¹⁹

Jedoch lassen sich auch noch weite Informationen aus den Verbindungsdaten ableiten: Interessen, Hobbys und Gewohnheiten, sogar Süchte und Sehnsüchte. Denn betrachtet man die VDS im Rahmen der Internet-Nutzung noch einmal gesondert, so wird klar, dass das Surf-Verhalten klare Rückschlüsse auf die Persönlichkeit zulässt²⁰. Wer zum Beispiel mehrmals die Woche auf einen Server

18 Bei Interesse lässt sich diese Abfrage durch „Stille-SMS“ (also durch inhaltslose „Service-SMS“, welche nur abgesendet werden um das Gerät zum veröffentlichen seines Standortes aufzufordern) auch automatisieren

19 Freiling, Felix C. (2009): Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung

20 Allein über die Art wie die Suchmaschine Google benutzt wird lässt sich das Geschlecht und das Alter, bis auf 5 Jahre genau mit einer hohen statistischen Wahrscheinlichkeit vorhersagen.

zugreift, auf dem ein Modellflug-Forum gehostet ist, wird sich mit hoher Wahrscheinlichkeit für Modellflugzeuge interessieren. Dieses Beispiel lässt sich durch deutlich sensitivere „Hobbies“ ersetzen.

Durch die Verkehrsdatenanalyse lassen sich also drei Arten von Informationen ableiten: Kommunikationsmuster, Bewegungsmuster und Persönlichkeitsprofile.

- **Entzugsmöglichkeiten**

Für Geheimnisträger (Regierungsbeamte, „Trader“ von Großbanken, Geheimdienstmitarbeiter) wurden in den vergangenen Jahrzehnten Systeme entwickelt, um sich der Verkehrsdatenanalyse entziehen zu können. Dabei werden zumeist einfache Geräte mit IMEI-Wechsler und multiplen Sim-Karten im Zusammenhang mit Zeittabellen verwendet – Personen einer bestimmten Gruppe sind also jeweils nur zu bestimmten Zeiten unter bestimmten Telefonnummern zu erreichen, welche nur kurze Zeit Gültigkeit besitzen.

Ein solches System lässt sich jedoch auch kostensparend mit einigen anonymen Sim-Karten (aus dem EU-Ausland) und einer begrenzten Anzahl von Handys (vom Flohmarkt oder Second-Hand-Geschäften) realisieren.

Ausschlaggebend ist nicht die Technik, sondern ein hohes Maß an Sorgfalt, sich genau an die Zeittabellen zu halten und niemals eine der Nummern für andere Zwecke zu verwenden.

Äquivalent dazu ist es möglich, sich der VDS bei Aktivitäten im Internet durch den Einsatz von Anonymisierungsdienste wie „Annon“ oder „TOR“ zu entziehen.

„Terroristen“ oder Personen aus dem Umfeld der Organisierten Kriminalität ist es also ein leichtes, unentdeckt zu bleiben, und die

Motivation sollte in solchen Kreisen hoch genug sein, um diese Mittel auch anzuwenden.

„Nur“ der Normalbürger bleibt im Überwachungsnetz kleben.

• **Kritik erster Ordnung**

Es muss angemerkt werden, dass einige Staaten in der EU die Richtlinie genutzt haben, um weit aus mehr zu speichern, als vorgesehen war, und dabei auch bewusst gegen europäische Datenschutzrichtlinien verstoßen: Nach einer Mitteilung der Europäischen Kommission aus dem Jahr 2010 ist in einigen Ländern nicht nur eine Speicherpflicht von 10 Jahren vorgesehen, es werden in einigen Staaten schon heute sogar Kommunikationsinhalte gespeichert, wie etwa E-Mail-Header. Bei Mobiltelefonaten erfassen die Behörden zum Teil nicht nur den Standort zum Beginn des Gesprächs, sondern zeichnen die Bewegungen des Nutzers kontinuierlich auf, um genauere Bewegungsprofile erstellen zu können.²¹

Die beiden stärksten und augenscheinlichsten Argumente für eine kritische Haltung gegenüber der VDS sind jedoch darin zu finden, dass erstens durch dieses Instrument das rechtsstaatliche Prinzip der Unschuldsvermutung unterlaufen wird und zweitens spezielle soziologische Schutzräume, welche sowohl im Grundgesetz als auch in der Rechtspraxis verankert sind, ihren Sonderstatus verlieren:

1) Die Kommunikation der Bürger wird ohne Anfangsverdacht überwacht. Niemand ist also mehr potentiell unschuldig – schon bevor auch nur ein Hinweis auf ein Fehlverhalten vorliegt, wird das Leben der Bürger überwacht.

²¹ Europäische Kommission (2010): Report 01/2010 on the second joint enforcement action

2) Genauso stark wiegt das Argument der Schutzräume. Würde die Politik versuchen die Schweigepflicht von Anwälten, Ärzten, Priestern und Seelsorgern abzuschaffen, würde sie von der Bevölkerung abgestraft. Der Bruch mit den Grundsätzen unserer Gesellschaft wäre offensichtlich. Die (redundante) Architektur der VDS (- es wird auf beiden Seiten der Verbindung gespeichert -) schafft diese soziologischen Schutzräume - die selbst auferlegte Weg-hör-Pflicht des Staates - jedoch faktisch ab. Kontaktaufnahmen zu Seelsorge-Telefonen, Ärzten, Priestern und Anwälten auf elektronischem Wege liegen durch die VDS offen.

2.2 Biometrie: Der neue „ePass“ und der „ePA“

• Definition

Die Biometrie beschäftigt sich generell mit Messungen an, bzw. von Lebewesen und den damit verbundenen Mess- und Auswerteverfahren.²²

Der Begriff wird häufig auf *biometrische Erkennungsverfahren* reduziert, welche jedoch zusammen mit der *biometrischen Statistik* (Entwicklung und Anwendung statistischer Methoden zur Auswertung von Messungen an lebenden Wesen) die beiden Hauptbereiche der Biometrie bilden. Für die Thematik dieser Bachelor-Arbeit sind beide Teilaspekte von Bedeutung. Diese Arbeit konzentriert sich im folgenden Abschnitt auf Erkennungsverfahren auf Grund biologischer Charakteristika, der Einfluss von Statistik wird in einem späteren Kapitel verhandelt.

• Hintergrund und Geschichte

Den Begriff der „Biometrie“ umweht häufig ein Hauch der Super-Moderne, jedoch wurde eines der ersten bekannten biometrischen Erkennungsverfahren schon 1879 entwickelt und basierte bereits auf 11 Körperlängenmaßen. Drei Jahre später legte Galton bereits den wissenschaftlichen Grundstein für die Nutzung des Fingerabdrucks als weiteres Merkmal.

Mittlerweile eignen sich unter anderem folgende Merkmale zur Personenidentifikation: Körpergröße, Verlauf der Iris, Fingerabdruck, Gesichtsgeometrie, Handgefäß- bzw. Venenstruktur der Hand, Handgeometrie, Nagelbettmuster, Körpergeruch und (als bekanntestes Merkmal) der „Genetischen Fingerabdruck“, generiert aus der DNA.

Elektronische Aufzeichnungen ermöglichen zusätzlich die Verwendung

²² Vgl. Wolchon, Marcus (2004): Konzeption und Implementation eines Authentifizierungssystems auf Basis von biometrischen Merkmalen und Transpondertechnologie

des Klangs der Stimme, des Herzschlags, des Ohrvolumens, des Tippverhaltens auf Tastaturen und den Gangstiels als personenspezifische Merkmale.

Jedoch können nur stark distinktive Charakteristika wie Iris und Zehnfingerprint eine zuverlässige Identifikation von Millionen von Menschen ermöglichen, weshalb diese beiden Merkmale, zusammen mit der Gesichtsgeometrie, am häufigsten Anwendung finden.

Bis vor wenigen Jahren wurde biometrische Personenidentifikation vornehmlich zum Schutz besonders sensibler Örtlichkeiten, wie zB. Forschungslabore oder militärischer Anlagen verwendet²³, sowie zur direkten Aufklärung von schweren Straftaten (Mord, Vergewaltigung) herangezogen. Seit einigen Jahren wird jedoch daran gearbeitet, jeden EU-Bürger biometrisch zu vermessen.

• **Gesetzliche und politisch-rhetorische Implementation**

Die Anfänge der biometrischen Vollerfassung der EU-Bürger geht zurück auf den 11. Dezember 2000 an dem das so genannte „EuroDAC“-System, eine Fingerabdruckdatenbank für Asylbewerber, beschlossen wurde. Das System, welches im Januar 2003 fertig gestellt wurde, soll verhindern, so das Vertragswerk, dass ein Asylbewerber in mehreren Mitgliedstaaten gleichzeitig einen Asylantrag stellt.²⁴ Man kann dies aber auch als erste Gewöhnungsphase interpretieren, durch welche die EU-Bürger daran gewöhnt werden sollten, dass es richtig sein könne, Menschen, welche keine Straftat begangen haben einer erkennungsdienstlichen Behandlung zu unterziehen, angeblich zum Wohle der Gesellschaft.

23 Jedoch wurde auch zB. die Eingänge des Zoos in Hannover so umgerüstet, dass Dauerkartenbesitzer durch Gesichtsgeometrie Zugang erhalten.

Vgl. Ziegler, Michael: Europas (2003): Größte Gesichtserkennungsanlage im Zoo Hannover

24 Europäische Kommission (2010): Asylum – a common space of protection and solidarity

Nachdem die USA damit gedroht hatten, die Visumsfreiheit für europäische Reisende aufzuheben, beschloss am 13. Dezember 2004 der Rat der Europäischen Union die Einführung eines neuen, EU-weit standardisierten, Reisepasses. In diesem wurden zum ersten mal maschinenlesbare biometrische Daten des Inhabers unter anderem Gesichts- und Fingerabdruckmerkmale, hinterlegt.²⁵ Die USA begründeten ihre Haltung gegenüber der EU mit der Gefahr des „internationalen Terrors“, welche durch nicht biometrisch vermessene Bürger gesteigert sei. Als das deutsche Bundeskabinett am 22. Juni 2005 den EU-Beschluss in nationales Recht überführte, schlug der federführende damalige Bundesinnenminister Otto Schily in dieselbe Kerbe. Er bezeichnete den „ePass“ als *„wichtigen Schritt auf dem Weg zur Nutzung der großen Fortschritte der Biometrie für die innere Sicherheit“*.

Auf der Informationshomepage des Bundesministerium des Innern, [„www.epass.de“](http://www.epass.de) wurde man noch deutlicher. Dort heißt es bis heute:

*„**Terroristen** und **Kriminellen** soll es nicht gelingen, mit gefälschten Reisedokumenten oder den echten Papieren einer Person, der sie besonders ähnlich sehen, einzureisen. [...] Die Mitgliedstaaten der Europäischen Union haben sich nach den **Anschlägen des 11. September 2001** auf die Einführung der Biometrie bei Pässen, Visa und Aufenthaltstiteln verständigt.“* (Hervorhebungen von mir)

Die Bundesregierung musste auf Anfrage jedoch nicht nur zugeben, dass der alte deutsche Reisepass als eines der sichersten Dokumente der Welt galt (mit nur sechs Totalfälschungen im Zeitraum 2001 bis 2006), sondern auch, dass noch nie Fälschungen deutscher Pässe im Zusammenhang von terroristischen Aktivitäten aufgetreten sind.²⁶

²⁵ Europäischer Rat (2004): Verordnung (EG) Nr. 2252/2004 des Rates, Brüssel

²⁶ Deutscher Bundestag (2007): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE – Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen

Noch erbärmlicher mutet die offizielle Argumentation an, wenn man berücksichtigt, dass die Anfänge des europäischen Reisepasses auf das Jahr 1997, also vier Jahre vor dem „Elften September“ 2001 zurückverfolgt werden können, als die ICOA, eine Unterorganisation der UN, damit beauftragt wurde, Standards für die Einführung von elektronisch auswertbaren biometrischen Merkmalen in Reisedokumenten zu definieren. Die Argumentation des „Terrors“ wurde nur nachträglich übergestülpt.

Um die Stimmen der Kritiker klein zu halten, wurde die Einführung des Reisepasses, inklusive biometrischem Lichtbild auf das Jahr 2005 gelegt, die Abgabe der Fingerabdrücke jedoch erst durch eine Gesetzesänderung 2007 verpflichtend. Des Weiteren wurde argumentiert, dass der Reisepass ja nicht verpflichtend sei, sondern dessen Beantragung auf Freiwilligkeit basiere. Für eine Person, die jedoch z.B. aus beruflichen Gründen auf gültige Reisedokumente angewiesen ist, ist diese Argumentation ein Schlag ins Gesicht.

Nachdem also in der zweiten Phase ein Teil der EU-Bevölkerung „freiwillig verpflichtet“ wurde, sich einer Behandlung zu unterziehen, welche vormals exklusiv für Verbrecher und dringend Tatverdächtige reserviert war, geht man jetzt dazu über, dieses Verfahren auf die gesamte Bevölkerung auszuweiten. Am 18. Dezember 2008 beschloss der Deutsche Bundestag die Einführung des neuen Personalausweises unter der damaligen Bezeichnung „ePA“ (elektronischer Personalausweis), welcher zum 1. November 2010 verpflichtend eingeführt wird. Mittlerweile sind die Behörden häufig dazu übergegangen (wahrscheinlich aufgrund der Proteste gegen den „ePass“), das neue Dokument als „nPA“ (neuer Personalausweis) zu bezeichnen. In dem neuen Personalausweis wurden weitestgehend dieselben Datenfelder implementiert wie im „ePass“: Das biometrische Gesichtsbild wird heute schon verpflichtend hinterlegt, die Abgabe der Fingerabdrücke des rechten und linken Zeigefingers ist noch freiwillig.

Mit einer Gesetzesänderung, linear kongruent zum „ePass“ ist jedoch zu rechnen.

Dafür spricht auch, dass der „ePA“ zusammen mit seinen europäischen Pendanten, unter dem Projektnamen „European Citizen Card“ (ECC - Spezifikation „CEN prTS 15480 - ECC05“)²⁷ bereits EU-weit definiert wurde, inklusive der Fingerabdrücke.²⁸

Auf Grundlage dieses Beschlusses, sowie der transatlantischen und globalen Schwesterprojekte ist davon auszugehen, dass Personalausweis und Reisepass auf lange Sicht der in der European Citizen Card zu einem einzigen Dokument verschmelzen werden.

• Erhobene Daten

Da sich „ePass“ und „ePA“ aus technischer Sicht kaum unterscheiden, werden beide Dokumente im Folgenden gemeinsam behandelt. Unterschiede sind gekennzeichnet.

Die beiden Dokumente verfügen über einen so genannten RFID-Funk-Chip, über welchen die dort gespeicherten Daten kontaktlos abgerufen werden können. Die verschiedenen Datengruppen werden dabei durch jeweilige Schutzmechanismen umschlossen.²⁹

Insgesamt sind 15 Datengruppen auf dem Chip angelegt. Die ersten beiden Datengruppen sind dabei redundant zu den „physischen“³⁰ Informationen, welche durch einen Menschen einfach abgelesen werden können³¹: Vorname, Nachname, Geburtsort und -datum,

27 Meister, Giesela / Daum, Henning (2009): Neue Sicherheitsmechanismen und Profile der European Citizen Card

28 Die zweite Version wurde 2010 in Zusammenarbeit von Fraunhoferinstitut und Sagem auf der CeBIT 2010 vorgestellt.

Vgl. Fraunhofer-Institut (2010): Fraunhofer auf der CeBIT 2010 - European Citizen Card 2.0

29 Diese im einzelnen zu erläutern und zu analysieren würde den Rahmen dieser Arbeit sprengen. Erste Anmerkungen befinden sich jedoch weiter hinten im Kapitel.

30 Auch elektronisch gespeicherte Daten sind physisch. Dennoch findet sich in der Fachliteratur diese Unterscheidung.

31 Beim „ePA“ sind diese Daten sogar doppelt redundant angelegt und befinden sich zusätzlich in der „MRZ“ (deutsch: „MLZ“ - „maschinenlesbare Zone“) am unteren Rand des Passes.

Wohnsitz (nur „ePA“) Geschlecht, Körperhöhe und Augenfarbe, sowie einer Unterschriftprobe und der Dokumentennummer (beim „ePass“ die Pass-Identifikationsnummer „PassID“, beim „ePA“ die Seriennummer).

Zusätzlich wird hier das Foto hinterlegt, welches darauf getestet wurde, dass es geometrisch (biometrisch) auslesbar ist und vor Ort ein biometrisches Gesichtsfeldbild aus den vorliegenden Daten errechnet werden kann. Die eigentliche Geometrie wird aus Speichergründen (noch) nicht hinterlegt. Die Firma Samsung wurde jedoch damit beauftragt, den „ePA“ so weiterzuentwickeln, dass auch ein rotierender 3D-Film der Gesichtsgeometrie hinterlegt werden kann. Auf der CES 2010 gab das Unternehmen seinen Erfolg bekannt und präsentierte das Ergebnis der Öffentlichkeit.³² Ob und wann dieses „Feature“ gesetzlich implementiert wird, ist zur Zeit nicht ersichtlich.

In der Datengruppe 3 werden die Fingerabdrücke hinterlegt.

Interessanterweise ist auch die Datengruppe 4 beim „ePass“ bereits benannt. Sie wurde für die Iris-Aufnahmen „reserviert“. Noch werden keine Iris-Bilder erhoben. Aufgrund des stark distinktiven Charakters der Iris, welches es ermöglicht, Millionen von Menschen noch präziser zu unterscheiden, sowie die Schaffung dieses bereits benannten Platzhalters, lassen jedoch nur den Schluss zu, dass die politische Implementation der technischen Implementation in Kürze folgen wird.

Des Weiteren wurden noch neun weitere Datengruppen (4 bis 15) implementiert. Diese werden für weitere, noch nicht definierte biometrische Merkmale freigehalten. Welche zusätzlichen Merkmale aufgenommen werden, steht zur Zeit noch nicht fest. Auszugehen ist jedoch davon, dass die Erhebung des Ohrvolumens aufgrund der einfachen Bestimmung mittels eines Handy-artigen Gerätes³³, zu den

³² Engadget Germany(2010): CES2010: Samsung integriert 3D-Animation im Personalausweis

³³ Gemessen wird hierbei die personenspezifische Ausbreitung von Schallwellen im menschlichen Ohr.

ersten zusätzlich erhobenen Datengruppen gehören wird, sowie einer Infrarot-Aufnahme des Ohres.³⁴

- **Kritik erster Ordnung**

„falscher“ Datenschutz:

Die auf den Dokumenten hinterlegten Daten sind standardisiert. Die Lesegeräte, welche es möglich machen, auf diese zuzugreifen, werden weltweit ausgeliefert, um den dortigen Behörden die Identifikation von EU-Bürgern zu ermöglichen. Dabei wird zwischen vertrauenswürdigen Staaten, welchen es möglich ist, auf alle eben verhandelten Datengruppen zuzugreifen, und Staaten, die nur autorisiert sind, die ersten beiden Datengruppen auszulesen, unterschieden. Diese Unterscheidung bleibt jedoch geheim. Dies schließt Krisenregionen und „failing states“ ausdrücklich ein.

Für den Reisenden ist also nicht erkennbar, ob der Staat, in den er ein- bzw. aus dem er ausreisen möchte, die Berechtigung hat, das Dokument allumfassend zu verwenden und den für das Auslesen der höheren Datengruppen benötigten zertifizierten Schlüssel erhalten hat.

Wird der Reisende nun aufgefordert, sich für eine Abnahme des Gesichtsfeldes vor einer Kamera zu positionieren oder die Hand auf ein Fingerabdrucklesegerät zu legen, kann dieser nicht einschätzen, ob nun seine Daten „nur“ mit denen auf dem Dokument abgeglichen werden oder ob diese von dem Staat eigenmächtig erhoben werden. Von außen ist nicht sichtbar, ob das Gerät die beiden Fingerabdrücke bzw. das Gesichtsbild vergleicht oder den Fingerabdruck/das Gesicht scannt und zusammen mit den (für den Staat lesbaren) Daten (PassID, Name, Geburtsdatum) in einer Datenbank ablegt.

³⁴ Dies könnte zu einer Verschmelzung von Videoüberwachung und Biometrie führen, da durch Infrarot-Aufnahmen Personen anhand ihrer Ohren auch über größere Distanzen mit bisher unerreichter Genauigkeit identifiziert werden können.

Es ist also möglich, dass Staaten, welche nicht einmal nach den europäischen Datenschutzstandards als „vertrauenswürdig“ einzustufen sind, biometrische Register über reisende EU-Bürger anlegen. Gleichzeitig kann auch nicht sichergestellt werden, dass auch Staaten, welche den Anforderungen formal genügen, die von ihnen überprüften Daten nicht permanent speichern.

Die deutschen Bürger werden also als „Reiseweltmeister“ ihre biometrischen Daten zwangsweise weltweit verteilen.

Der RFID-Funkchip und die Sicherheitsimplementation:

RFID steht für „radio-frequency identification“ - Das System beruht also auf einem Chip ohne Stromversorgung, welcher, wird er in der richtigen Frequenz angesprochen, die Funkwellen nutzt, um Berechnungen durchzuführen (z.B. sich zu Identifizieren, oder gespeicherte Daten auszulesen) und diese mit Hilfe der (kurzzeitig) gespeicherten Energie wieder zurücksendet.

Ursprünglich war dem System nicht angedacht „geheime“ Daten zu speichern oder zu verarbeiten. Zwischen 1944 und 2005 wurden jedoch nicht nur etwa 2,397 Milliarden RFID-Chips verkauft³⁵ sondern auch die Technologie diesbezüglich weiterentwickelt.

Eines der bekanntesten und erfolgreichsten Systeme, welche RFID zur vertraulichen Kommunikation, etwa zur Zugangsberechtigung von Gebäuden benutzt ist „Mifare“. Hierbei werden die Daten durch den Einsatz von Kryptographie verschlüsselt. Das weltweit sowohl von Unternehmen als auch von Staaten verwendete System galt lange Jahre als unangreifbar und wurde deshalb exzessiv eingesetzt. Am 13. April 2008 gelang es einer Forschergruppe den Algorithmus zu analysieren und grundlegend zu brechen.^{36 37} Am 29. Dezember

³⁵ Das, Raghu (2005): RFID tag sales in 2005 - how many and where

³⁶ Courtois, Nicolas / Nohl, Karsten / O'Neil, Sean (2008): Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards

³⁷ Zum damaligen Zeitpunkt wollte weder der Hersteller noch eine staatliche Organisation den Bruch der Verschlüsselung bestätigen, selbst als am selben Tag alle Benutzer der Londoner U-bahn auf einmal umsonst fahren konnten - da das auf MIFARE basierende Zahlungssystem „Oystercard“ alle

desselben Jahres wurde dann ein Programm veröffentlicht, das es auch Laien möglich macht, die Verschlüsselung zu umgehen.

Dass die im „ePass“ und „ePA“ verwendeten Systeme zu einem großen Teil auf der „MIFARE“-Technologie basieren stimmt bedenklich.

Generell muss jedoch im Falle der Kryptographie generell herausgehoben werden, dass es meistens nicht nötig ist ein System als solches zu korrumpieren (das System als Ganzes zu verstehen und somit *jeden* Schlüssel errechnen zu können), sondern wesentlich effizienter der gerade vorliegende Schlüssel angegriffen werden kann (diesen einen Schlüssel *erraten*). Der beim „ePass“ verwendete Schlüssel wird aus dem Vor- und Nachnamen, dem Geburtsdatum und dem Ablaufdatum des Passes errechnet. Insgesamt hat der Schlüssel nur 56bit, ist aber aus den eben genannten Gründen nicht besonders „stark“, da sowohl das Geburtsdatum als auch das Ablaufdatum nur aus Zahlen besteht, wovon die jeweils die Hälfte der Ziffern mit einfachem Menschenverstand zu erraten ist.³⁸

Die Überwindung dieser Hürde ist mit Hochleistungsrechnern in immer kürzerer Zeit zu bewältigen, und auch der Zeitpunkt, zu dem ein junges Talent das System als solches kippen wird, ist der Erfahrung nach nicht allzu weit in der Zukunft anzusiedeln.

Die Gegenargumentation, zumindest gegen den Angriff auf den speziellen Schlüssel lautet, dass das Dokument auf eine „Lesereichweite“ von 10cm spezifiziert ist - ein Angreifer müsste sich seinem Opfer sehr stark nähern, um die Rechenoperationen durchführen zu können.

Kunden mit Freifahrten beschenkte.

Die indirekte Bestätigung erfolgte jedoch in den darauf-folgenden Tagen durch das holländische Innenministerium. Dieses ließ ihre Gebäude sowie mehre Gebäude der Geheimdienste kurzzeitig vom Militär umstellen und ihre (auf „MIFARE“ basierenden) Zugangssysteme komplett austauschen – Die Behörde verwies dabei auf gravierende Sicherheitsmängel.

³⁸ Vor- und Zuname bestehen nur aus Buchstaben. Das Ablaufdatum ist auf 10 Jahre begrenzt und muss in der Zukunft liegen. Ein Datum besteht des Weiteren aus einer Zahl zwischen 1 und 12, dann einer Zahl zwischen 1 und 31 und dann noch einer Zahl, zwischen 1910 und dem aktuellen Jahr. Die Kombinationsmöglichkeiten sind also stark eingegrenzt, der daraus errechnete Schlüssel durch reines Ausprobieren „schnell“ findbar.

Die Reichweite einer pro-aktiven Antenne ist jedoch nur davon abhängig, welche Energie man dieser entgegenschickt. Der 10cm-Radius, in dem es möglich sein soll, das Dokument auszulesen, bezieht sich auf TÜV-geprüfte Sendestationen. Mit einem einfachen Lötkolben, einem Stück Draht und etwas technischem Verständnis lässt sich jedoch deren Leistung vervielfachen.³⁹ So können Lesereichweiten von vielen Metern erzielt werden. Die konstruierte Situation, in einer Fußgängerzone auf Pass-Jagd zu gehen, ist also deutlich realistischer als ursprünglich angenommen.

Neben diesem „aktiven“ Auslesen des Dokumentes ist es möglich die Kommunikation passiv mitzuhören. So beschreibt der Chaos Computer Club in einer sicherheitstechnischen Analyse des „ePasses“:

„Passives Abhören bedeutet, daß der Angreifer die offizielle Kommunikation zwischen dem Paß und dem Lesegerät (zum Beispiel an der Grenze) mithört. Dieses ist bis zu 30 Metern und unter Laborbedingungen sogar schon bis zu 50 Metern möglich.

Es sollten also auch die Personenkraftwagen, die vor dem Flughafen warten, beobachtet werden .„⁴⁰

Durch die oben geschilderte Situation könnten also, genauso wie in der Szenerie der Fußgängerzone, entweder unerlaubte Register angelegt werden oder auch komplette Pass-Fälschungen vorgenommen werden.⁴¹

Noch einfacher als das Erraten eines Schlüssels ist es jedoch, seine Zutaten exakt zu kennen. Da alle benötigten Daten auf den Pass aufgedruckt sind, reicht eine einfache Fotokopie des Passes, wie sie zum Beispiel bei Hotelbuchungen täglich Millionenfach geschieht.

³⁹ Ein Personenkreis, der über die kriminelle Energie zum Fälschen von Pässen, bzw. zum unerlaubten Auslesen und Kopieren von Ausweisdokumenten besitzt, wird sich wohl kaum an TÜV-Richtlinien für Funkantennen halten.

⁴⁰ Chaos Computer Club (2005): Spass mit dem ePass, S.5f

⁴¹ Dies bezieht sich natürlich nur auf den elektronischen Teil des Dokumentes.

Die kryptographischen Schutzmechanismen, welche die Sensiblen Daten schützen sollen, sind im Falle des „ePA“ etwas ausgefeilter (nicht aus den aufgedruckten Daten zu errechnen und auch technisch deutlich versierter), generell gelten jedoch alle bisher geschilderten elektronischen Angriffsszenarien auch bei diesem Dokument als prinzipiell durchführbar.

Der nicht-biometrische Bürger:

Die in den beiden Dokumenten verwendeten biometrischen Verfahren beziehen sich auf eine Art biometrischen Otto-Normal-Bürger. Eine nicht geringe Anzahl von Menschen können jedoch von den Systemen nicht richtig erfasst werden.

So haben laut der BIOSIC Studie von 2004 11% der erwachsenen Bevölkerung (Deutschlands) dermatologische Probleme, welche eine Abnahme der Fingerabdrücke unmöglich macht. Hinzu kommt, dass die Abtastfähigkeit der Hautfaltungen auf den Fingerkuppen mit steigendem Lebensalter deutlich abnimmt. Ein Großteil der Rentner wird also nie in den „Genuss“ eines verwendbaren biometrischen Fingerabdrucks kommen.

Aber auch ganze Berufsgruppen sind von dem Verfahren ausgenommen, wie etwa Chemiker, die durch ihre Arbeit häufig an ihren Fingerspitzen „Tiefe verlieren“, was ebenfalls dazu führt, dass keine Abdrücke genommen werden können. Dies trifft auch auf andere, stark handwerklich orientierte Berufsgruppen zu.⁴²

Ähnlich verhält es sich bei der Gesichtsbiometrie. Menschen mit Spasmen oder Lähmungen der Gesichtsmuskulatur oder Kinderlähmung sind generell von dem Verfahren ausgenommen, da

⁴² Bundesamt für Sicherheit in der Informationstechnik (2005): „Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen –BioP II“

ein „neutrales Gesichtsbild“ nicht angefertigt werden kann.

Das derzeit verwendete Verfahren scheitert zusätzlich an Menschen mit „Eierköpfen“ (also Menschen mit einem „langem Gesicht“), an Menschen deren Augen im Vergleich zur Kopfbreite „zu nahe“ zusammen liegen, sowie an kleinwüchsigen Menschen, die unter 1,55m groß sind. Hinzu kommt eine Schwäche des Systems für Hornbrillen und „*starker Gesichtsbehaarung*“.⁴³

Unabhängig davon, ob man diesen zweistelligen Prozentsatz der Bevölkerung, welcher von den Systemen nie richtig erkannt werden wird, als signifikant anerkennt oder nicht, ist nicht bestreitbar, dass Menschen aufgrund ihrer genetischen Veranlagung oder ihrer Biographie durch den Einsatz der biometrischen Verfahren in zwei Klassen eingeteilt werden. Die „biometrischen Bürger“ dürften Grenzen oder Personenkontrollen deutlich schneller hinter sich bringen als die Bürger zweiter Klasse, welchen jedes mal eine Sonderbehandlung zu teil wird.

Redundante Gültigkeit

Da der angebliche Sicherheitsgewinn immer als wichtigstes Argument für die Einführung der elektronisch gespeicherten biometrischen Daten herhalten müsste, könnte man vermuten, dass diese für die Gültigkeit der Dokumente ausschlaggebend sein müssten.

Dem ist jedoch nicht so. Die Dokumente bleiben auch dann noch gültig, wenn der Chip, bzw. die Antenne beschädigt ist, und damit ein Auslesen der hinterlegten Daten nicht mehr möglich ist.

Die Identifikationsfunktion sei auch dann noch gegeben, durch bloßes Ablesen der aufgedruckten Daten, so das Innenministerium.

Möchte man den Behörden nicht unterstellen, dass die erhobenen biometrischen Daten zentral gespeichert werden, sondern, wie

43 Ebd.

angegeben nach der Herstellung des Passes vernichtet werden, so verbirgt sich der Sinn der Datenerhebung. Ein Fälscher kann alle Sicherheitsmechanismen, welche durch die Implementation des Chips gewonnen werden sollten durch die Verwendung einer defekten Antenne umgehen. Ein zusätzlicher Sicherheitsgewinn ist also durch die biometrische Vollerhebung der Bevölkerung nicht erkennbar.

An dieser Stelle sei auch angemerkt, dass das Argument der schnelleren elektronischen Verarbeitung hinfällig wird, wenn man beachtet, dass der EU-Reisepass seit 1988 und der Bundespersonalausweis seit 1987 maschinell lesbar ausgestellt wird.

Intressenskonflikte

Die Bundesdruckerei war ehemals ein „bundeseigenes Unternehmen“ wurde jedoch im Jahr 2000 privatisiert. Danach erlebte der Betrieb eine neunjährige Phase mit ständigem Wechsel der Eigentümer. Dabei geriet die Bundesdruckerei mehrfach in die Hand ausländischer Unternehmen. Erst 2009 zog der Bund die Notbremse und ließ den Betrieb von verschiedenen Landesbanken zurückkaufen. Ob in der Zwischenzeit jedoch sensible (biometrische) Daten an andere Staaten oder (europäische) Interessengruppen weitergegeben wurden, sollte jedoch nicht Spekulationsobjekt von Verschwörungstheoretikern bleiben, sondern eingehend geprüft werden.

Vermischung hoheitlicher und nichthoheitlicher Funktionen

Des Weiteren wird gelegentlich kritisiert, dass auf dem „ePA“ hoheitliche Funktionen und nichthoheitliche Funktionen vermischt werden.

So soll der Wirtschaft mit dem Personalausweis auch ein Werkzeug an die Hand gegeben werden, welches diese für ihre Belange benutzen kann.

Vorgesehen ist unter anderem, dass Unternehmen Daten auf dem

staatlichen Dokument des Bürgers speichern können.⁴⁴ Eine eingehende Betrachtung dieser Entwicklung (- der Verschmelzung von Staat und Wirtschaft und der damit einhergehenden Entstaatlichung von Macht -) kann im Rahmen dieser Arbeit jedoch nicht geleistet werden.

Hier sei nur angemerkt, dass diese „Features“ auf Grund der hohen Kosten der Umgebungstechnologie in nächster Zukunft wohl kaum Anwendung finden werden.

• **Entzugsmöglichkeiten**

Um - entweder aus krimineller Absicht, oder um ein „gültiges“ Dokument trotz körperlicher Defizite zu erhalten - fehlerhafte biometrische Daten in die Dokumente einschleusen zu können, sind keine speziellen Fertigkeiten oder Vorrichtungen von Nöten.

Falsche Fingerabdrücke können etwa mit Hilfe einiger Haushaltsutensilien, einer Digitalkamera und etwas Theaterkleber selbst hergestellt werden. Mit Hilfe eines seit 2006 im Netz zirkulierenden Video⁴⁵ ist es jedem Leihen möglich, auf die Finger aufklebbare Attrappen zu produzieren, die von dem System nicht erkannt werden.

So wurden in den letzten Jahren unter anderem sowohl frei erfundene Fingerabdrücke erfolgreich in Pässe eingeschleust als auch Fingerabdrücke deutscher Politiker.

Noch einfacher, aber deutlich schmerzhafter, ist das Entfernen der eigenen Fingerabdrücke, etwa mit Hilfe von starken Säuren wie Batteriesäure, was zu einer Ausstellung eines Dokumentes mit dem Vermerk „keine Fingerabdrücke“ führt.

Das System der Gesichtsfeldgeometrie ist genauso fehleranfällig. „Getestet“ von Bürgern, denen im ersten Anlauf auf Grund der weiter

44 Plötz, Henrik (2009): Die Technik des neuen ePA

45 Chaos Computer Club (2005): Anleitung Fingerabdruck fälschen

oben beschriebenen körperlichen „Unzulänglichkeiten“ (Augen zu nahe zusammen, „Eierkopf“) ein Dokument verwehrt wurde, zeigte sich schnell, dass das verwendete System gegen einfache Manipulation der Bilder mit Hilfe eines Bildbearbeitungsprogrammes nicht gerüstet ist. Die Bürger gingen also dazu über, ihr eigenes Foto so weit zu stauchen oder zu stecken, bis es den Systemanforderungen genügte. Eine Übereinstimmung mit der tatsächlich lebenden Person kann auf diese Weise jedoch nicht mehr erzielt werden.

Neben dieser einfachen Manipulation lässt sich das System noch weit aus deutlicher angreifen. Die Gesichtsbilder werden komprimiert abgespeichert. Unabhängig von der eigentlichen „Datendichte“ des Bildes wird hierfür eine Version erzeugt, die einer maximalen Speichergröße entspricht. Durch das Einschleusen von Bild-Fraktalen kann der Kompressionsalgorithmus jedoch so weit in die Knie gezwungen werden, dass aus dem errechneten Bild keine verwendbaren Daten re-extrahiert werden können.

Zusammenfassend kann nur eine ähnliche Schlussfolgerung wie bei der Vorratsdatenspeicherung gezogen werden: Mit genügend krimineller Energie können die Systeme sehr einfach umgangen werden, der normal-sterbliche Bürger steht jedoch einem starken Eingriff in seine Grundrechte gegenüber, gegen das er sich wohl eher im seltenerem Fall wehren wird.

2.3 Recht am eigenen Bild: „Nacktscanner“

- **Definition**

Nacktscanner, auch „Körperscanner“ genannt, sind Systeme mit denen, mit Hilfe von schwacher Röntgenstrahlung oder Terahertzstrahlung, die Oberfläche des menschlichen Körpers abgebildet werden kann. So sollen unter der Kleidung versteckte Gegenstände sichtbar gemacht werden. Bis vor wenigen Jahren wurden die Kontrollsysteme vornehmlich am Eingang zu sensiblen Bereichen verwendet, sind mittlerweile jedoch an immer mehr Flughäfen im Einsatz.

- **Gesetzliche und politisch-rhetorische Implementation**

Die ersten Systeme wurden in den USA und in Israel angewendet – in der Europäischen Union sind die Geräte eigentlich (noch) nicht zugelassen. Einige Staaten haben sich jedoch Sondergenehmigungen zu „Testzwecken“ zuteilen lassen, darunter die Niederlande und Großbritannischen. Deutschland will im Herbst 2010 in Hamburg einen „Versuchsaufbau“ starten.

Dabei wird auf einen „Sicherheitsgewinn“ verwiesen – darauf, dass die Systeme „Waffen“ und „Sprengstoffe“ finden könnten - ein ausdrücklicher Verweis auf die angebliche „Terrorgefahr“ bleibt hierzulande jedoch zumeist aus. Die Politik hält sich in Deutschland weitestgehend zurück und überlässt das Feld zum größten Teil der Gewerkschaft der Polizei, welche jedoch in den vergangenen Monaten unterschiedliche Signale gesendet hat, die Testreihen aber generell unterstützt.⁴⁶

Um die europäische Presse wohlwollend zu stimmen, organisierte der Europäische Polizeikongress eine Begleitausstellung zum Thema Nacktscanner, welche damit beworben wurde, dass es

⁴⁶ Gewerkschaft der Polizei (2010): Gesamte Flugsicherheit muss auf den Prüfstand

Pressefotografen möglich sein sollte, „Lara-Croft-Lookalikes“ beim Durchschreiten der Systeme fotografieren zu können.⁴⁷

• Erhobene Daten

Die Systeme erzeugen eine Art Nacktbild, zumeist in 2D, weiter entwickelte Anlagen in 3D. Dabei wird die Hautoberfläche, bzw. die Rückstahlfläche der spezifischen Strahlung, fototechnisch verarbeitet. Hierbei ist es unerheblich, ob auf einem etwaigen angeschlossenen Monitor ein Strichmännchen oder der nackte Körper in seiner vollen Pracht wiedergegeben wird.⁴⁸ Die Erzeugung eines Nacktbildes ist dabei systemimmanent.

Die meisten Systeme enthalten offiziell sowohl Speichermöglichkeiten als auch Schnittstellen, durch welche aufgenommene Bilder abgerufen werden. Auch die anderen Systeme beherbergen jedoch systembedingt zumindest temporäre Speichereinrichtungen, und nicht beschriebene Schnittstellen können nur durch eine Offenlegung des Quellcodes ausgeschlossen werden - wogegen sich jedoch ein Hersteller aus Gründen der Wirtschaftsspionage immer stellen wird.

Kein Anbieter kann also wirklich dafür garantieren, dass die aufgenommenen Nacktbilder nicht missbräuchlich verwendet werden. Mittlerweile sind dahingehend auch einige Fälle bekannt geworden, verschiedene Anbieter aber auch verschiedene Behörden wurden der Falschinformation überführt.^{49 50} Im August 2010 etwa gab der „United States Marshal Service“, eine Art US-Bundespolizei, zu, mehrere Zehntausend Scan-Bilder gespeichert zu haben.⁵¹ Keiner dieser Fälle ereignete sich jedoch in der EU.

47 Europäischer Polizeikongress (2010): Globale Sicherheit – Herausforderungen für Europa

48 Das Problem der Minitorabstrahlung wird in einem späteren Kapitel verhandelt.

49 Knoke, Felix (2010): Nachtscanner erhalten doch Speichermöglichkeiten

50 Zetter, Kim (2010): Airport Scanners Can Store, Transmit Images

51 Declan McCullagh, Florian Kalenda (2010): US-Bundespolizei speichert Nacktscannerbilder

• Entzugsmöglichkeiten

Es ist möglich, sich dem „Sinn“ der Systeme zu entziehen - der Entblößung selbst kann jedoch nur entronnen werden, indem Orte vermieden werden, an denen diese Systeme zum Einsatz kommen.

Der „Sinn“ meint hier, dass die Entdeckung von versteckten Gegenständen etwa durch auf den Körper aufgeklebte Fleischteile (Schnitzel) verhindert werden kann. Die Geräte können aufgrund ihrer Funktionsweise nicht zwischen körpereigenem Gewebe und Fremdgewebe unterscheiden. Schon ein mit Klebeband befestigtes Schnitzel überlistet die automatisierten Systeme, ein mit Theaterkleber und etwas Hingabe präparierter Mensch sollte auch die manuelle Bildabnahme überstehen.

Ferner ist es beliebten Personen möglich kleinere Gegenstände einfach zwischen „Speckfalten“ zu klemmen. Auch sich im Körper befindende Objekte, geschluckte Objekte, können zu meist nicht sichtbar gemacht werden.

• Kritik erster Ordnung

Der Bürger muss beim Durchschreiten des Scanners das Recht auf das eigene Bild abgeben. Gleichzeitig wird durch den Vorgang sehr plastisch in seine Intimsphäre eingegriffen.

2.4 Überwachung durch nicht-staatliche Akteure am Beispiel „Kundenscoring“

Neben den bisher vorgestellten, staatlich verankerten Technologien kann auch in einem anderen Zusammenhang von der Überwachung des Bürgers gesprochen werden. Auch hier geht es um die Stärkung der eigenen Position durch Wissen.

Beispielhaft hierfür steht das so genannte „Kundenscoring“, welches im Folgenden erläutert wird:

• Definition

„Kundenscoring“ ist ein Prinzip, welches in seiner ursprünglichen Form zuerst in der Bankwirtschaft unter dem Begriff „Kreditscoring“ angewendet wurde.

Beim „Kreditscoring“ handelt es sich um ein mathematisches System, bei welchem aufgrund von vorliegenden Daten und mit Hilfe einer statistischen Analyse ein Zahlenwert errechnet wird, welcher die Kreditwürdigkeit einer Person (oder eines Unternehmens) repräsentiert.⁵²

Auf Grund von der persönlichen Eigenschaften (wie etwa Beruf, Arbeitgeber, Familienstand, etwaige negative Schufa-Einträge) einer Person und seiner wirtschaftlichen Verhältnissen (verfügbares Einkommen und Vermögensverhältnisse) möchte die Bank so ihr Risiko bei der Kreditvergabe statistisch vorhersagen können.

Dieses auf Punkten („Scores“) beruhende System wurde in den letzten Jahren von vielen Wirtschaftszweigen adaptiert und erweitert.

Neben den bisher verwendeten Daten werden hier häufig (zusätzlich zu den Kontaktmöglichkeiten, wie Telefonnummer und Mail-Adresse) Merkmale wie „Geschmack“ und „Interessen und Hobbys“, „Buchkäufer“, „Autofahrer“, „Raucher“ etc hinzugefügt. So erweitert sich nicht nur der Datenbestand sondern auch die Möglichkeiten der Dienstleistungen und damit der Kreis der Interessenten:

Unternehmen können nun nicht mehr nur die Kreditwürdigkeit ihrer *vorhandenen* Kunden ausleuchten, sondern auch die *potentieller* Kunden, sowie Informationen über deren Eigenschaften, Vorlieben und Kaufverhalten. So können etwa Adressen-Listen der Zielgruppe des Marktsegmentes maßgeschneidert erworben werden.

⁵² Vgl.: Pamitzke, Thomas (2003): Kreditscoring unter Stichprobenselektion zur Erlangung des Grades eines Diplom-Kaufmanns

Immer häufiger wird auch die Beziehung zum Kunden auf Grund von „Kundenscoring“ beeinflusst, etwa in der Qualität der jeweiligen Kundenbetreuung.

In den letzten Jahren ist branchenübergreifend ein florierender Datenhandel entstanden. Daten aus immer mehr Quellen werden zusammengetragen und verkauft. Je mehr Merkmale über eine Person zusammen getragen werden können, desto wertvoller wird der Datensatz und desto mehr potentielle Abnehmer findet dieser.

- **Gesetzliche und politisch-rhetorische Implementation**

Eine reale gesetzliche Implementation dieser Vorgänge hat nicht stattgefunden, die Praxis beruht in weiten Teilen auf weit zurückliegend entstandenen Gesetzen. Die auf Grund der informationstechnischen Revolution entstandenen Veränderungen wurden von der Gesellschaft in weiten Teilen noch nicht erkannt – eine gesellschaftliche und damit auch politische Diskussion beginnt erst zur Zeit.

- **Erhobene Daten**

Die Systeme basieren auf unterschiedlichen Algorithmen mit unterschiedlichen und unterschiedlich vielen Merkmalen. Jedes Merkmal wird statistisch verwertet, sowohl hinsichtlich der Kaufkraft und Kreditwürdigkeit als auch der „Einkaufswahrscheinlichkeit“ für bestimmte Produkte und Dienstleistungen, aber auch statistischen Größen wie „Erkrankungswahrscheinlichkeit“ oder „Betreuungsbedarf“.

Welche Daten hierbei verwendet werden, ist also primär abhängig von dem Vorhandensein bestimmter Daten. Erhoben werden die Daten häufig durch so genannte „Direktmarketing-Umfragen“, Gewinnspiele und Kundenbefragungen, aber auch durch die Verwendung

öffentlicher Daten, wie dem Mietschlüssel.

Liegen Daten für eine bestimmte Person nicht vor, wird häufig ein statistischer Rückgriff auf möglichst „gleiche“ Merkmalsträger vorgenommen. So werden etwa Durchschnittseinkommen für ganze Straßenzüge oder Stadtviertel errechnet.

- **Kritik erster Ordnung**

Im Gegensatz zur Schufa-Abfrage erfolgt die Abfrage von Kundenscoring-Werten ohne Kundeneinverständnis. Nur die initiale Erhebung, sowie der Erst-Verkauf, ist gesetzlich reglementiert.

Da in den meisten Fällen weder die verwendeten Scoring-Algorithmen noch die verwendete Datengrundlage offen gelegt wird, ist nicht ersichtlich ob nicht auch (entwendete) Daten, welche etwa durch staatliche Überwachung generiert wurden oder nicht zur Datenweitergabe bestimmt waren, für die Verfahren herangezogen werden.

Für den Kunden ist nicht nachvollziehbar, welche Daten von welchem Akteur weitergegeben wurden und wie aktuell diese sind, bzw. ob diese überhaupt wahrheitsgemäß erhoben wurden.

Auch kann argumentiert werden dass die Reduktion einer Person auf einen statistischen Wert als unmenschlich anzusehen ist.

3. Die fragmentierte Datenmacht

Nachdem aufgezeigt wurde, welche Daten in welchen Zusammenhängen erhoben werden, soll nun, um deren Wirkung auf die Gesellschaft einordnen zu können, im folgenden Kapitel die Eigenheiten elektronische Daten - und deren Wirkungszusammenhänge in einem größeren Maßstab - betrachtet werden.

3.1 Daten

- **Begriffsdefinition: Daten**

Nach DIN 44300 Teil 2-2.1.13 sind Daten *„Gebilde aus Zeichen oder kontinuierliche Funktionen, die aufgrund von bekannten oder unterstellten Abmachungen, und vorrangig zum Zweck der Verarbeitung, Informationen darstellen.“*⁵³

Oder anders ausgedrückt: **Daten sind gruppierte Informationseinheiten.**

Daten enthalten Informationen - diese können jedoch nie für sich selbst stehen. Nicht der Inhalt selbst definiert eine Information zum Datenelement, sondern erst die *„bekannten oder unterstellten“* Verknüpfungsmöglichkeiten.

Der Satz: „Erika ist am Bahnhof“ birgt sicherlich Information in sich. Der Empfänger muss dem Satz jedoch einen Sinn zuordnen können. Dabei muss erkannt werden, dass es sich bei „Erika“ um eine (ggf. bekannte) Person handelt und das „Bahnhof“ wohl eine Ortsbezeichnung darstellt.

⁵³ Binder, Jörg (1993): Strafbarkeit intelligenter Ausspähen von programmrelevanten DV-Informationen

In der elektronischen Datenverarbeitung könnte dieser Zusammenhang wie folgt ausgedrückt werden:

Bekannte Abmachung: [o]=Ort; [p]=Person

Datum: o=Bahnhof;p=Erika

• Daten und ihr Fortpflanzungsmechanismus

Jedoch muss beachtet werden, dass nicht jede Information, welche aus einer bestimmten Datengruppe extrahiert werden kann sofort ersichtlich ist.

Unterstellt man, dass zu den beiden oben genannten „gruppierten Informationen“ in einer anderen Datenbank weitere Informationen hinterlegt sind, wie etwa die Schuhgröße von „Erika“, so kann daraus extrahiert werden, dass eine Frau mit der Schuhgröße X am Bahnhof war. Dies funktioniert, auch wenn zu keinem vorangegangenen Zeitpunkt der Bahnhof mit einer Schuhgröße verknüpft war.

Oder plastischer ausgedrückt:

Gibt es eine Datenbank, in welcher alle Menschen aufgeführt sind, welche grüne Augen haben, sind diese momentan nur durch diesen Zusammenhang gruppiert.

Stellte sich jedoch eines Tages heraus, dass Menschen mit grünen Augen häufiger straffällig würden, so wäre eine neue Gruppierung entstanden ohne dass dabei dem ursprünglichen Datenbestand („Menschen mit grünen Augen“) etwas hinzugefügt werden müsste.⁵⁴ Person „X“ wäre jetzt also potentiell gewaltbereiter, aufgrund des ursprünglichen Merkmales „grüne Augen“.

Die Verknüpfung von Gewaltbereitschaft und Augenfarbe muss nicht bei der Erhebung intendiert sein. Einer gruppierten Information können also weitere Informationen hinzugefügt werden, welche die

⁵⁴ Man könnte auch argumentieren, dass sich die Abmachung geändert hätte, jedoch sind (bekannte) Abmachungen wiederum nur „gruppiert Informationen“

anderen Informationen neu bewerten, selbst wenn diese Bewertung nur für *einen* gruppierten Teil angelegt ist.

Daten können durch Verknüpfung also „Daten-Kinder“ gebären.

Jedes Datum kann potentiell mit jedem Datum verknüpft werden. Die Aussagekraft eines Datenbestandes kann also immer nur für einen jeweiligen Zeitpunkt angenommen werden.

3.2 Kontrollverlust der Kontrolle

- Elektronische Datensicherheit im Allgemeinen und im staatlichen Raum

Jeder der jemals ein elektronisches Datenverarbeitungssystem über einen gewissen Zeitraum verwendet hat, wie etwa den heimischen PC oder den Arbeits-Laptop, wird früher oder später mit der Erfahrung konfrontiert, dass diese Systeme selbst bei absolut sachgemäßem Gebrauch fehleranfällig sind. Es hat noch nie ein „sicheres System“ gegeben, und kann es auch nie geben.⁵⁵

Dies bezieht sich sowohl auf die eigentliche Funktion des Systems, also auch auf dessen Sicherheit bezüglich von „Datenverlusten“, etwa durch Eindringen von Schadsoftware oder aktives, manuelles Eindringen durch Angreifer.

Um jedoch zumindest die Funktion des Systems dauerhaft zu gewährleisten, sind die meisten Systeme redundant aufgebaut - so sind etwa verschiedene Zugriffsmechanismen implantiert oder die Daten werden an anderer Stelle zusätzlich vorgehalten.

Dies erhöht jedoch die Möglichkeit des „Verlierens“ der Daten im zweiten Sinne, der Habhaftwerdung der Daten durch Andere.

⁵⁵ Dieses Prinzip kann aus der Funktionsweise der Systeme bzw. den zugrunde-liegenden elektronischen und logischen Basismechanismen erklärt werden und ist selbst-explikativ.

Beim Aufbau eines Datensystemes wird eine Abwägung zwischen dem Nutzen des Systems auf der einen Seite und den Kosten der ständigen Systemerneuerung, der Einbruchswahrscheinlichkeit und den Kosten, welche beim Verlust der Daten entstehen andererseits, abgewogen.

Dieser „Security-Trade“, der bei jeder Datenverarbeitungstechnologie abgewogen werden muss, unterläuft im Falle der meisten bisher beschriebenen Technologien jedoch das in diesem Umfeld als Steuerung vorausgesetzte marktwirtschaftliche Sicherungsprinzip:

Während z.B. Banken täglich damit konfrontiert sind, bekannt gewordene Sicherheitsmängel in ihren Systemen hinsichtlich des potentiellen wirtschaftlichen Schadens (sowie der damit korrespondierenden Image-Einbußen) zu bewerten, dies mit der Eintrittswahrscheinlichkeit des Schadensfalles zu verrechnen und dieses Ergebnis mit den Kosten zu vergleichen, die nötig wären, das System an dieser Stelle sicherer zu machen, steht der Bürger im Falle einer Bekanntgabe seiner persönlichen Daten ein Verlust gegenüber, der sich nur schwer durch finanzielle Mittel kompensieren lässt.

Veröffentlichte persönliche Daten sind veröffentlicht und können in den meisten Fällen nie wieder eingefangen werden.

Durch das, den oben beschriebenen Systemen häufig anhaftende, Kompetenz-Wirrwarr wird häufig auch eine Situation geschaffen, in der die Zuordnung der Verantwortung schwer fällt. Haftet etwa im Rahmen der VDS im Verlustfall der Provider, da die Daten bei ihm aufbewahrt wurden, oder die Strafverfolgungsbehörden, da sie die einzigen waren, welche legal darauf zugreifen durften, der eingesetzte Sicherheitsmitarbeiter, oder etwa das BSI, da dieses das System lizenzierte?⁵⁶

⁵⁶ Es sei ausdrücklich erwähnt, dass dieses Phänomen auch an den anderen Beispielen wie etwa den „Nacktscannern“ oder der Videoüberwachung, aber auch an Hand von (elektronischen) Krankenakten oder Hartz VI-Anträgen, durchexerziert werden kann.

Auch der Konkurrenzdruck, welcher dem Security-Trade-Modell immanent ist, kann in den meisten Fällen nicht aufgebaut werden, es sei denn, man behauptet, der „Kunde“ - also der Bürger - habe die Möglichkeit, den „Anbieter“ zu wechseln: Er stehe also vor der Wahl, sich das Land auszusuchen und falls es ihm „hier“ nicht gefalle, könne er sich ja ein anderes suchen.

• **„Klassische“ Datenverluste in der näheren Vergangenheit**

In den letzten Jahren gab es immer wieder bedeutende Datenverluste. So erregte nicht nur die unter dem Stichwort des „Datenstollens“ bekannt gewordene Verlustgeschichte der Deutschen Telekom AG oder das unerlaubte Ausspähen von Bankkonten durch Mitarbeiter⁵⁷ Aufmerksamkeit, sondern auch Datenverluste staatlicherseits von deutlich größeren Ausmaßen wie etwa bei den englischen Behörden, welche zugeben mussten, 25 Millionen persönliche Datensätze verloren zu haben⁵⁸ oder den unter der Bezeichnung der „war diaries“ bekannt gewordenen Einsatzdaten der US-Armee, welche nun öffentlich im Netz zu finden sind.

• **Datenverlust am Beispiel der Monitorabstrahlung**

Neben diesen offensichtlichen Datenverlusten, welche zumeist auf eine unsachgemäße Behandlung der Daten, oder auf ein direktes Kompromittieren des Systems zurückzuführen ist, können auch so genannte „Seitenkanalattacken“ zu Datenverlusten führen.

Die dabei plastische Möglichkeit wurde nach dem Entdecker dieser Schwachstelle, dem niederländischen Forscher Wim van Eck als „Van-Eck-Phreaking“ benannt, taucht jedoch auch häufig unter dem Namen „TEMPEST“ (- einem Programm der NSA⁵⁹, welches sich van Ecks

57 Webermann, Jürgen (2010): Datenskandal bei der Hamburger Sparkasse?

58 Tagesspiegel, der (2007): Daten-Skandal weitet sich aus,

59 National Security Agency (1972): TEMPEST: a signal problem – The story of the discovery of various compromising radiations from communications and Comsec equipment

Erkenntnisse zu Nutzen machte -) in der Fachliteratur auf.

Alle elektrischen Geräte senden aufgrund ihrer Bauweise (- der Verwendung von Strom -) elektromagnetische Wellen aus. Diese sogenannte „kompromittierende Abstrahlung“ kann mit geeigneten Empfangsgeräten über sehr große Entfernungen hinweg aufgefangen werden. Ohne Hindernisse wie Hausmauern gelangen Abhöraktionen mit einem Abstand von über hundert Metern, innerhalb von Gebäudekomplexen sind die möglichen Distanzen etwas kürzer.

Dabei sendet jedes Gerät ein gerätespezifisches Signal, durch welches diese voneinander unterschieden werden können. Gleichzeitig gibt das Gerät jedoch durch Modulation auch bekannt, was gerade auf / in ihm passiert. So ist es etwa möglich durch die Abstrahlsignatur den Datenverkehr einer Signalleitung abzuhören. Dies ist technisch jedoch sehr anspruchsvoll und häufig werden bei äußerst sensiblen Datenströmen Störsender angebracht, um zu die Daten zu schützen.

Jedoch teilen auch Monitore ihrer Umgebung mit, was gerade auf ihnen dargestellt wird. So kann ein Angreifer aus den empfangenen Daten das Videosignal rekonstruieren und auf einem eigenen Bildschirm darstellen, oder einfach automatisiert speichern und verarbeiten.⁶⁰

• **Daten-Akteure**

Um die bisher gewonnenen Erkenntnisse zu strukturieren, ist es sinnvoll, die Akteure voneinander abzugrenzen. Dabei ist zu

⁶⁰ Diese Erkenntnis war unter anderem ausschlaggebend für die Entscheidung des Bundesverfassungsgerichts Wahlcomputer in Deutschland generell skeptisch zu betrachten. Dem OVG war es gelungen, für eine angeforderte Stellungnahme für das höchste deutsche Gericht in einem Testaufbau zu beweisen, dass es möglich ist, noch aus einem Nachbargebäude nachzuvollziehen für welchen Kandidaten ein „Wähler“ so eben seine Stimme abgegeben hatte. Vgl. hierzu: Bundesverfassungsgericht(2009): BVerfG, 2 BvC 3/07

beachten, dass die Bezeichnungen nicht immer trennscharf voneinander abgegrenzt werden können, sondern ein und dasselbe Subjekt in mehreren Rollen auftreten kann.

Eine Person, eine Behörde, Interessengruppe oder ein Unternehmer, welche Daten erhebt oder aufbereitet, wird im Folgenden als „**Sammler**“ bezeichnet. Hierbei wird davon ausgegangen, dass die Daten auf legalem Wege erhoben werden.

Ein handelndes Subjekt, welches die Daten „unerlaubt“ erhebt oder in einem Sinn verwendet, welches dem ursprünglichem Zwecke der Datenerhebung widerspricht, wird als „**Täter**“ bezeichnet. Dies bezieht sich dabei sowohl auf einen Datendiebstahl, als auch auf eine nachträgliche Gesetzes-, bzw. Bestimmungsänderung - also einer Überführung der Daten in einen anderen Interpretationszusammenhang.

Es wird dabei zwischen sowohl zwischen „**Erhebungstätern**“, welche Daten illegal erheben, und „**legalistischen Tätern**“, die „berechtigterweise“ die Daten einer neuen Bestimmung zuführen, unterschieden, als auch zwischen „**Innentätern**“, also Personen die etwa Daten an ihrem Arbeitsplatz „mitgehen lassen“, und „**Außentätern**“, also etwa „Hackern“ welche in ein System eindringen.

Eine Person, eine Behörde, Interessengruppe oder ein Unternehmer, welche anfallende Daten besitzt, zusammenführt oder diese verarbeitet, wird im folgenden als „**Wissender**“ bezeichnet.

Dabei ist es unerheblich, ob dem „Wissenden“ jegliche Aussagekraft der Daten bewusst ist oder nicht und auch, ob die Daten auf legalem oder illegalem Wege erhoben, bzw. zusammengeführt worden sind.

- **Langzeitwirkung von Daten**

In der Fachliteratur (meistens innerhalb der Disziplin der Informatik) taucht hin und wieder eine Begebenheit auf, die die bisher dargestellten Zusammenhänge sehr plastisch aufzeigt.

Jedoch spielt die Geschichte in verschiedenen Publikationen in verschiedenen Ländern und, damit korrespondierend, schwankt der Zeitpunkt der Handlung auch um ein, zwei Jahre. Es lässt sich auch kein Verweis auf die Primärquelle finden.⁶¹

Daher wird die Geschichte nun im Sinne einer Parabel eingeführt, da diese unabhängig von ihrem Wahrheitsgehalt alle bisher besprochenen Elemente anschaulich verortet.

Dabei muss ausdrücklich vermerkt werden, dass es nicht darum geht, die berüchtigte „Nazi-Keule“ zu schwingen, sondern dass die Parabel in leicht veränderter Form, genauso gut in einer (dystropischen) Zukunft angesiedelt werden könnte.

Als zum Beginn des zwanzigsten Jahrhunderts Rundfunkgeräte in Mode kamen, begann auch der Staat sich dafür zu interessieren, welche Haushalte mit dieser neuen Technologie ausgestattet wurden. teils zum Zwecke der Erhebung von Steuern, zum Teil aus einfachem Interesse. Die dabei erhobenen Daten wiesen in ihrer Art und ihrem Umfang starke regionale Unterschiede auf.

1933 übernahmen die Nazis die Herrschaft in Deutschland und überzogen kurze Zeit später Europa mit Krieg. Der Holocaust begann, und alle Juden des Kontinents waren in Gefahr.

Um die jüdische Bevölkerung zu schützen, und ihnen die Möglichkeit zu geben, unerkannt unterzutauchen, vernichteten etliche Landesväter und Bürgermeister der umliegenden Länder die vorhandenen Personenregister.

61 Es wird daher auch im Rahmen dieser Arbeit diesbezüglich auf Quellenangaben verzichtet.

3. Die fragmentierte Datenmacht

Jedoch fielen den Nazis in bestimmten Fällen die Rundfunkregister in die Hände. Wenn auf diesen, neben anderen Daten, wie etwa der Haushaltsgröße inklusive dem Geschlecht der einzelnen Personen, auch die Religionszugehörigkeit vermerkt war, so konnten die Besatzer Personen jüdischen Glaubens sehr viel einfacher ausfindig machen.

Der eigentliche „Sammler“ in dieser Geschichte ist also wohl ein übereifriger Beamter, der niemandem schaden wollte. Den Besatzern wurde durch seine Arbeit jedoch ein Werkzeug an die Hand gegeben, zu „Wissenden“ zu werden, in dem sie (als „Täter“) die Daten in einen neuen Zusammenhang eingliederten.

- **Zwischenfazit**

Daten werden in verschiedenen Handlungszusammenhängen erhoben, wenn es um Überwachung geht. Dabei wird es durch ständige Vernetzung immer schwerer vorauszusagen, welche Daten „intim“ sind, da auch durch die Neugruppierung nicht-intimer Daten intime Daten entstehen können.

Einmal erhobene Daten sind nur sehr schwer wieder einzufangen.

4. Gesellschaft unter Kontrolle?

Im anschließenden Kapitel wird nun diskutiert werden, wie sich Überwachung auf die Gesellschaft auswirkt. Hierbei wird zuerst die Reaktion des Einzelnen in den Fokus gerückt, um anschließend gesamtgesellschaftlich diskutiert zu werden.

4.1 Auswirkungen der Überwachung auf den Einzelnen

- **Persönlichkeitsentwicklung**

Der Umgang mit, und auch die Abgrenzung von „überwachten Räumen“ und „Privatsphäre“ - also nicht-überwachte Räume - ist in der (westlichen) Gesellschaft ein wichtiger Teil des Inkulturationsprozesses.

So sind schon Dreijährige in der Lage, verschiedenen Personen unterschiedliche Regelwerke zuzuordnen und, damit korrespondierend, deren „Überwachungsgrad“ zu internalisieren: Was man bei Opa darf, ist bei Mama noch lange nicht erlaubt, und Opa schaut weg, wenn man Süßigkeiten nascht.

Der Drang, sich selbst zu erleben, nicht-überwacht zu agieren, sich auszuprobieren um neue Erfahrungen zu generieren, setzt zur selben Zeit ein. Dies treibt nicht nur Eltern junger Sprösslinge regelmäßig an den Rand der Verzweiflung, etwa beim Anblick der Marmeladebeschmierten Tapeten, sondern ist auch Voraussetzung für das Erlernen von Verantwortung. Nur durch eigenständiges, nicht-überwachtes Handeln kann auch Verantwortlichkeit internalisiert werden. Nur wenn die Konsequenz einer Handlung eigenverantwortlich erfahren wird, sind langfristige Steigerungen des Erkenntnishorizonts zu verwirklichen.

Der Drang sich zumindest zeitweise in nicht-überwachten Räumen aufzuhalten, ist zudem anscheinend tief in uns verwurzelt. So lieben es Kinder im Kindergartenalter aus Decken, Sofas und Einrichtungsgegenständen „Burgen“ bzw. „Höhlen“ zu bauen und stundenlang in ihnen zu spielen. Diese erste „plastische“ Darstellung einer Privatsphäre wird im Jugendalter weiterentwickelt und äußert sich etwa durch das immer stärkere Verteidigen der Machthoheit des eigenen Kinderzimmers, des Tagebuches und der (mittlerweile zumeist elektronischen) Korrespondenz, aber auch im für Jugendliche so typischen Cliquen-Verhalten, durch welche eine Art temporäre Gegenkultur geschaffen wird, die Erwachsene (die Überwacher) ausdrücklich ausschließt.

Diese nicht-überwachten Handlungsspielräume werden dabei genutzt, um die eigene Persönlichkeit zu entwickeln und verschiedene Persönlichkeits-komponenten „auszutesten“. Insbesondere ist es der heranwachsenden Persönlichkeit möglich, selbst zu entscheiden, welche bisher von außen angetragenen Regeln umgesetzt werden sollen. Durch die auf Interaktion basierenden Gruppenprozesse werden dabei neue Regelwerke geschaffen, welche selbstverantwortlich eingehalten, sanktioniert und weiterentwickelt werden.

Mit fortschreitendem Lebensalter wird der Grad der Privatheit einer Situation, im Zusammenhang mit Örtlichkeiten und (potentiell) anwesenden Akteuren, immer gradueller abgestuft. Das sichere Bewegen in beiden Räumen wird zur Routine.

Jedoch zeigt sich, dass auch eine ausgereifte Persönlichkeit auf Überwachung reagiert. Ein am Max-Planck-Institut durchgeführtes Experiment mit 96 Freiwilligen zeigte, dass die Anwesenheit eines „Überwachers“ auch bei Erwachsenen zu Verhaltensänderungen führen kann.⁶² Auch wenn in die Überwachung hier explizit durch die

⁶² Burnham, Terence; Hare, Brian (2005): Engineering Human Cooperation -Does Involuntary Neural Activation Increase Public Goods Contributions?

Anwesenheit eines „Gesichtes“ operationalisiert wurde, lassen sich die Erkenntnisse auf andere Überwachungszusammenhänge übertragen. Nicht umsonst geben Konzerne Millionen für Mitarbeiter-Monitoring aus.

Dies lässt sich auch anhand der Selbst-Disziplinierung nachweisen: Ein Manager, der ein zu erfüllendes Ziel vor seinen Kollegen öffentlich schriftlich fixiert hat, wird signifikant höhere Anstrengungen an den Tag legen um dieses Ziel auch zu erreichen.⁶³

Abstinenz von Überwachung führt zu (Eigen-)Verantwortung. Gleichzeitig ist es dem Prinzip eines sozialen Vertragswerkes inhärent, dass Regeln (positiv und negativ) sanktioniert werden müssen. Überwachung soll die Einhaltung dieser Regeln kontrollieren. Es muss also immer ein Gleichgewicht zwischen Überwachung und Nicht-Überwachung gefunden werden.

• **Die Rechte des Einzelnen**

Neben den juristisch formulierten Rechten des Einzelnen lassen sich aus den bisherigen Erörterungen zwei grundlegende Rechte ableiten: Das Recht aus Fehlern zu lernen und, damit korrespondieren, das Recht allein-gelassen zu werden.

Wie weiter oben beschrieben, ist es für die Persönlichkeitsentwicklung relevant, auszuprobieren. Dies schließt etwaige Fehlentscheidungen ausdrücklich mit ein. Diesbezüglich hat sich eine gesellschaftliche Norm des absichtlichen Vergessens etabliert, welche etwa unter dem Stichwort der „Jugendsünden“ im alltäglichen Sprachgebrauch wiederzufinden ist.

Dieses absichtliche Vergessen geht einher mit einem absichtlichen Nicht-Hinschauen. Beides kann im Sinne dieser Arbeit als

63 Gaycken, Sandro / Constanze Kurz (2008): 1984.exe, S. 73ff

„ostentatives Nicht-Wissen“ zusammengefasst werden. Dieses „right to be left alone“⁶⁴ welches bereits 1980 formuliert wurde, kann durchaus als Menschenrecht interpretiert werden. Denn durch Überwachung „ [...] leidet die freie Entfaltung, die jedem Bürger innerhalb freiheitlich-demokratischer Grenzen zusteht, unter dem Eindruck, auf Schritt und Tritt potentiell für immer sichtbare Spuren zu hinterlassen.“⁶⁵

Diese Freiheit, keine Aufzeichnungen zu hinterlassen, wird durch die (elektronische) Überwachung eingeschränkt. Noch stärker wiegt jedoch das Argument, dass durch die im dritten Kapitel beschriebenen Eigenschaften von elektronischen Daten der bisher in unserer Gesellschaft gültige „Vergessenshorizont“ unterlaufen wird.

• Reaktion des Einzelnen am Beispiel von „Promis“

Welche Auswirkungen ein starker Überwachungsdruck auf den Einzelnen hat, lässt sich sehr plastisch am Beispiel der so genannten „Promis“ studieren. Gemeint sind hier Personen, die, zumeist auf Grund ihrer herausgehobenen Arbeit (Schauspieler, Staatsoberhäupter, Musiker), oder aufgrund eines medialen Ereignisses, plötzlich (oder allmählich), sehr stark in der Öffentlichkeit stehen und von den Medien „überwacht“ werden.

In diesem Zusammenhang kommt es häufig zu einer Entgrenzung der sonst gültigen sozial verhandelten Trennlinien zwischen Privatem und Öffentlichem. So musste schon der eine oder andere „Promi“ feststellen, dass er 24 Stunden am Tag von Reportern verfolgt wird, sein Grundstück vor niemandem mehr sicher ist und alltägliche Handlungen öffentlich diskutiert werden.

64 Brandeis, Louis / Warren, Samuel (1890): „The Right to Privacy“, in: Harvard Law Riview, Vol4, S. 139-220

65 Aus der Urteilsbegründung des Bundesverfassungsgerichts zur Volkszählung. Vgl. Bundesverfassungsgericht (1983): 1 BvR 209/83 [et. al]

Betrachtet man das Verhalten dieser „Überwachungsoffer“, so ist häufig ein starker Hang zur Überkonformität festzustellen.

Diese findet sich jedoch in verschiedenen Ausprägungen wieder, sowohl in der Komplettübernahme des zugelegten Rollenbildes (etwa des „Krawallmachers“, der „Diva“ oder des „Rock´n´Roll-Stars“), als auch in dem diametral gelagerten Versuch, die aktuellen Moral- und Wertvorstellungen komplett einzuhalten - selbst wenn diese nur noch oberflächlich in der Gesellschaft verankert sind, und es zur gesellschaftlichen Realität gehört, diese im Privaten zu brechen.

Hierbei ist ausdrücklich zu erwähnen, dass sich diese Verhaltensweise nicht nur auf die Vermeidung tatsächlicher Verletzungen der gesellschaftlichen Normen bezieht, sondern auch auf Handlungen, welche als Vorstufen oder Indizien gewertet werden könnten.

Eine Person, welche einem starken Überwachungsdruck ausgeliefert ist, neigt also stärker dazu, sich selbst zu spielen. Der Einzelne verliert dabei seine Individualität und wird zum Schauspieler einer ihm auferlegten Rolle. Dies geht einher mit dem Verlust von Eigenständigkeit und Selbstbestimmung, aber vor allem zu Lasten der Freiheit des Probierens und Sich-Selbst-Erfindens - also der freien Persönlichkeitsentfaltung.

4.2 Auswirkungen der Überwachung auf die Gesellschaft

- **Die freiheitliche demokratische Grundordnung**

Sind die bisher aufgezeigten Entwicklungen mit den Grundsätzen unserer Gesellschaft vereinbar?

Die Kernstruktur, welche unserer Gesellschaft zu Grunde liegt, wird als „freiheitlich demokratische Grundordnung“ bezeichnet und wurde vom Bundesverfassungsgericht in einer seiner ersten Entscheidungen, basierend auf dem Grundgesetz, wie folgt konkretisiert:

„Freiheitliche demokratische Grundordnung im Sinne des Art. 21 II GG ist eine Ordnung, die unter Ausschluss jeglicher Gewalt und Willkürherrschaft eine rechtsstaatliche Herrschaftsordnung auf der Grundlage der Selbstbestimmung des Volkes nach dem Willen der jeweiligen Mehrheit und der [1]**Freiheit und Gleichheit** darstellt. Zu den grundlegenden Prinzipien dieser Ordnung sind mindestens zu rechnen: die Achtung vor den [2]**im Grundgesetz konkretisierten Menschenrechten, vor allem vor dem Recht der Persönlichkeit auf Leben und freie Entfaltung**, die Volkssouveränität, [3]**die Gewaltenteilung**, die [4]**Verantwortlichkeit der Regierung**, die Gesetzmäßigkeit der Verwaltung, die Unabhängigkeit der Gerichte, das Mehrparteienprinzip und die [5]**Chancengleichheit für alle politischen Parteien mit dem Recht auf verfassungsmäßige Bildung und Ausübung einer Opposition.**“

BVerfGE 2, 1, 12

– Hervorhebungen sowie deren Nummerierung von mir

• Gefahren für die Gesellschaft

Welche Gefahren für eine Gesellschaft, die auf der freiheitliche demokratischen Grundordnung fußt, können also aus den bisher gewonnen Erkenntnissen extrahiert werden?

Zu1: Ob die *Freiheit* in ihrem vollen Umfang durch Überwachung angegriffen wird, ist nicht pauschal zu beantworten. Jedoch ist der Grundsatz der *Gleichheit* mit Zunahme der Daten über den Einzelnen immer stärker in Gefahr. Eine Gesellschaft, welche sich in eine Gruppe der „Wissenden“ und der „Nicht-Wissenden“ unterscheiden lässt, ist nicht mehr „gleich“. Den Wissenden liegt eine Datenmacht

zu Füßen, die es ihnen ermöglicht, Macht über die Nicht-Wissenden auszuüben - etwa durch Androhung der Veröffentlichung von Geheimnissen, aber auch durch bloße Anwendung von Herrschaftswissen.

Zu2: In welchem Umfang die *Menschenrechte* durch Überwachung in Gefahr sind, hängt vor allem von der jeweilig verwendeten Technik ab. Im Falle der Biometrie kann z.B. argumentiert werden, dass das Recht auf das eigene Bild verletzt wird.

Noch folgenschwerer ist jedoch das Argument zu verorten, dass das *Recht auf informationelle Selbstbestimmung* durch jede Art der Überwachung verletzt wird. Dies geht einher mit einem Verlust an Eigenständigkeit und Selbstbestimmung.

Das *Recht auf freie Entfaltung* wird mit dem Verlust der nicht-überwachten Räume stark angegriffen. Diese Entwicklung wird durch den Verlust des Vergessenshorizonts beschleunigt.

Zu3: Auch der Grundsatz der *Gewaltenteilung* ist mit zunehmender elektronischer Überwachung in Gefahr: Daten, welche eigentlich klar der geheimdienstlichen Sphäre zugeordnet werden können, werden immer häufiger in einem strafrechtlichen Zusammenhang verwendet.

Zu 4: Der Grundsatz der *Verantwortlichkeit* setzt sich unter anderem aus der *Verhältnismäßigkeit* und der *Wahl der geeigneten Mittel* zusammen.⁶⁶ In vielen Fällen kann hinterfragt werden, ob das Prinzip der Verhältnismäßigkeit im Falle der umfassenden Datenerhebungen eingehalten wird. An den in dieser Arbeit verhandelten Beispielen wird zudem schnell ersichtlich, dass die Mittel oftmals kaum geeignet sind, die eigentlichen Ziele der Überwachung zu erfüllen.

Zu 5: Nach dem Willen der Väter (und Mütter) des Grundgesetzes soll unsere Gesellschaft das Produkt konkurrierender Gesellschaftsideen

66 Bundesverfassungsgericht (2010): 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

sein, welche in ihrer jeweiligen Ausprägung unter anderem durch Parteien repräsentiert werden. Dabei wird die *Chancengleichheit* einer *Opposition* noch einmal ausdrücklich herausgestellt.

Steigen jedoch, durch einen sehr starken Überwachungsdruck, die Opportunitätskosten - welche entstehen wenn man sich der allgemein vorherrschenden Meinung nicht anschließen möchte - wird dieses Gleichheitsprinzip ausgehebelt.

Durch Überwachung wird nicht nur die Weiterentwicklung der Gesellschaft gehemmt und diese ihrer Innovationskraft beraubt, der Bürger verliert auch die moralische Verbundenheit zu dem Staat - da er nicht mehr im vollen Umfang als konstituierendes Objekt der Gesellschaft eintreten kann. Dies geht oftmals einher mit dem Verlust an Achtung für das Gesetz und die Vollzugsbehörden.

5. Gesellschaft am Scheideweg

Unsere Gesellschaft steht also tatsächlich am Scheideweg – und wohin die Reise geht, ist noch nicht abzusehen.

Die Veränderungen, die mit der alltäglichen technischen Überwachung Einzug in unsere Realität halten, sind so fundamental, dass das Versäumen einer umfangreichen gesamtgesellschaftlichen Diskussion verheerende Folgen haben könnte. Die Rolle des Staates muss überdacht und neu verhandelt werden. Aber auch das Rollenverständnis des Bürgers benötigt in diesem Zusammenhang eine neue Definition.

Gleichzeitig bleiben viele Vektoren ungewiss. Ob die Gesellschaft demnächst einer weiteren Spaltung unterliegt – „Wissende“ gegen „Überwachte“ – wird vor allem von der Kompetenz der Überwacher abhängen:

Denn unter Nudisten ist keiner nackt, und sind Daten aller einmal für jedermann abrufbar, so steht die Macht, welche sich aus diesem Wissen extrahieren lässt, potentiell allen offen.

Diesem Gedanken muss jedoch ein weiterer folgen: Eine (datentechnische) Spaltung der Gesellschaft, hinsichtlich der Kompetenz diese Daten auch zu nutzen, wird dadurch noch wahrscheinlicher: Auf der einen Seite die Technisch-versierten, auf der anderen Seite die Unbegabten. Jedoch sei in diesem Zusammenhang erwähnt, dass der „mündige Bürger“, welchen das Grundgesetz stets vor Augen hat, mindestens genauso selten vorkommt wie der Daten-mündige.

Und wie bei allen vorhergehenden Konflikten wird es Menschen mit genügend Kapital immer möglich sein, Vorteile aus allem zu ziehen.

Die Entwicklung wird also vor allem zu Lasten der Armen und „Dummen“ gehen.

Die Frage muss also lauten: Wo *wollen* wir als Gesellschaft hin?

Ist es von uns allen gewollt, dass wir Techniken einführen, die zwar auf der einen Seite kaum die Ziele erfüllen, unter welchen sie eingeführt wurden, andererseits, bezüglich ihrer Auswirkungen von den meisten Bürgern nicht verortet werden können?

Ist die Aufgabe der Privatsphäre zugunsten von mehr Sicherheit richtig? Lässt sich die Sicherheit auf diese Weise erhöhen? Ist es überhaupt die Aufgabe des Staates diese Art von Sicherheit zu gewährleisten?

Aber, man könnte die Fragen, welchen wir uns alle demnächst stellen müssen, auch noch deutlich weiter fassen:

Welche unserer Grundsätze sind nicht verhandelbar? Die Freiheit? Das Recht allein gelassen zu werden? Das Recht Fehler zu begehen, die einen nicht bis zum Lebensende verfolgen?

Und trägt der „Internationale Terrorismus“ - falls es ihn gibt - nicht den Sieg davon, wenn wir anfangen unsere Grundwerte derart zu veräußern?

Alle diese Fragen müssen in nächster Zeit von unserer Gesellschaft beantwortet werden.

Die Realität, an welcher sich unsere Entscheidung ausrichten wird, hängt unter anderem davon ab, wie viel Wissen dabei von denen beigesteuert wird, die nicht davon leben, ein aufgeschrecktes Wahlvolk mit immer neuen Terrormärchen zu versorgen – also von der Wissenschaft.

Und ein faktenbasierter Diskurs kann unserer Gesellschaft nur gut tun. - Fangen Sie an, forschen Sie los.

Abkürzungsverzeichnis

ePA	elektronischer Personalausweis
ePass	elektronischer Pass
IMAP	Internet Message Access Protocol - eMail-Zugriffs-Protokoll
IMEI	International Mobile Equipment Identity - Endgerätenummer für Mobiltelefone
IMSI	International Mobile Subscriber Identity - Identifikationsnummer der Sim-Karte
RFID	radio-frequency identification - (passive) Identifizierung mit Hilfe elektromagnetischer Wellen
SIM/Sim	Subscriber Identity Module - Chipkarte zur Nutzeridentifikation
SMTP	Simple Mail Transfer Protocol - Einfaches E-Mail-Sendeverfahren
TOR	The Onion Router - Netzwerk zur Anonymisierung der Verbindungsdaten
UMTS	Universal Mobile Telecommunications System - Mobilfunkstandart
VDS	Voratsdatenspeicherung
WAP	Wireless Application Protocol – spezielles Funknetzprotokoll

Literaturverzeichnis

Binder, Jörg (1993): Strafbarkeit intelligenten Ausspähens von programmrelevanten DV-Informationen, Tectum Verlag, Marburg

Bundesverfassungsgericht, Karlsruhe

(1952): BVerfGE 2, 1

(1983): 1 BvR 209/83 [et. al]

(2009): BVerfG, 2 BvC 3/07

(2010): 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08,

Bundesamt für Sicherheit in der Informationstechnik (2005):

„Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen –BioP II“, Bonn

Burnham, Terence; Hare, Brian (2005): Engineering Human Cooperation -Does Involuntary Neural Activation Increase Public Goods Contributions?, Max Planck Institute for Evolutionary Anthropology / University of Harvard:

<http://www.fas.harvard.edu/~ped/events/seminar/media/BurnhamHare.pdf>

Abgerufen am 03.05.2010

Brandeis, Louis / Warren, Samuel (1890): The Right to Privacy, In: Harvard Law Riview, Vol4, Harvard

Cappel, Christian (2006): Anachronismus einer „Drittwirkung“ - Das kognitivistische Konzept Karl-Heinz Ladeurs und die Matrix Gunther Teubners im grundrechtstheoretischen Spannungsfeld, Vittorio Klostermann, Frankfurt am Main

Chaos Computer Club (2005): Spass mit dem ePass, In: Datenschleuder 87, Pinguin Druck, Berlin

Chaos Computer Club (2005): Anleitung Fingerabdruck fälschen,

Berlin: <http://www.youtube.com/watch?v=OPTzRQNHzi0>

Abgerufen am: 14.05.2010

Courtois, Nicolas / Nohl, Karsten / O´Neil, Sean (2008):

Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards, University College London:

<http://eprint.iacr.org/2008/166.pdf>

Abgerufen am 03.05.2010

Das, Raghu (2005): RFID tag sales in 2005 - how many and where, IdtechX, Cambridge:
http://www.idtechex.com/research/articles/rfid_tag_sales_in_2005_how_many_and_where_00000398.asp
Abgerufen am 15.03.2010

Declan McCullagh, Florian Kalenda (2010): US-Bundespolizei speichert Nacktscannerbilder, Zdnet Deutschland, München:
http://www.zdnet.de/news/wirtschaft_sicherheit_security_us_bundespolizei_speichert_nacktscannerbilder_story-39001024-41535841-1.htm
Abgerufen am 12.08.2010

Deutscher Bundestag (2006): Plenarprotokoll 15/157, Bundestagsdrucksache 15/4597, Berlin

Deutscher Bundestag (2007): Plenarprotokoll 16/124, Bundestagsdrucksache 16/5875 , Berlin

Deutscher Bundestag (2007): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE – Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen, Drucksache 16/5228, Berlin:
<http://dipbt.bundestag.de/dip21/btd/16/055/1605507.pdf>
Abzurufen am: 8.08.2010

Engadget Germany(2010): CES 2010 - Samsung integriert 3D-Animation im Personalausweis:
<http://de.engadget.com/2010/01/07/ces-2010-samsung-integriert-3d-animation-im-personalausweis-mi/>
Abgerufen am: 13.02.2010

Europäische Kommission (2010): Report 01/2010 on the second joint enforcement action, 00058/10/EN WP 172, Direktorat C, Brüssel

Europäische Kommission (2010): Asylum – a common space of protection and solidarity, Brüssel:
http://ec.europa.eu/homeaffairs/policies/asylum/asylum_intro_en.htm
Abgerufen am: 30. 07. 2010

Europäischer Rat (2004): Verordnung (EG) Nr. 2252/2004 des Rates, Brüssel

- Europäischer Polizeikongress** (2010): Globale Sicherheit – Herausforderungen für Europa, Berlin:
http://www.daten.european-police.eu/police_programme.pdf
Abgerufen am: 15.08.2010
- Europäisches Parlament** (2006): Richtlinie 2006/24/EG Des Europäischen Parlaments und des Rates, Amtsblatt der Europäischen Union, Brüssel
- Europarat** (2001): Übereinkommen über Computerkriminalität - Bereinigte Übersetzung zwischen Deutschland, Österreich und der Schweiz abgestimmte Fassung, Budapest:
<http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm>
Abgerufen am: 10.06.2010
- Foucault, Michel** (1976): Überwachen und Strafen. Die Geburt des Gefängnisses, Suhrkamp, Frankfurt am Main
- Fraunhofer-Institut** (2010): Fraunhofer auf der CeBIT 2010 - European Citizen Card 2.0, Berlin:
http://www.fraunhofer.de/presse/cebit/European_Citizen_Card_2.0.jsp
Abgerufen am: 12.08.2010
- Freiling, Felix C.** (2009): Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, Technischer Bericht Universität Mannheim, Institut für Informatik
- Gewerkschaft der Polizei** (2010): Gesamte Flugsicherheit muss auf den Prüfstand, Berlin:
<http://www.gdp.de/gdp/gdp.nsf/id/p100101>
Abgerufen am: 11.07. 2010
- Gaycken, Sandro / Constanze Kurz** (2008): 1984.exe, transcript-Verlag, Bielefeld
- Hill, Werner** (1998): Erfassen, löschen und vernichten – Der Mensch in der Datei. In: Mitteilungen 162, Humanistische Union, Berlin
- Knoke, Felix** (2010): Nachscanner erhalten doch Speichermöglichkeiten:
<http://www.spiegel.de/netzwelt/web/0,1518,671491,00.html>
Abgerufen am: 23. 07. 2010
- McLuhan, Marshall** (1992): The Global Village: Transformations in World Life and Media in the Twenty-First-Century, Oxford University Press, Oxford

Meister, Giesela / Daum, Henning (2009): Neue Sicherheitsmechanismen und Profile der European Citizen Card, Giesecke&Devrient, München

Motti, Tiziano/ Záborská, Anna (2010): Schriftliche Erklärung zur Schaffung eines europäischen Frühwarnsystems gegen Pädophilie und sexuelle Belästigung, Europäisches Parlament, Brüssel

National Security Agency (1972): TEMPEST: a signal problem – The story of the discovery of various compromising radiations from communications and Comsec equipment, Cryptologic Spectrum, Vol. 2, No. 3

Parnitzke, Thomas (2003): Kreditscoring unter Stichprobenselektion, Berlin:
<http://edoc.hu-berlin.de/master/parnitzke-thomas-2003-07-30/PDF/parnitzke.pdf>
Abgerufen am: 23.06.2010

Plötz, Henrik (2009): Die Technik des neuen ePA, In: 26C3: Here be Dragons, Berlin

Pritlove, Tim (2007): GSM Hacking - Aufbau, Funktionsweise und Sicherheitsmängel von GSM-Netzwerken, Chaoradio Express, Ausgabe 56, Berlin

Schönherr, Maximilian (2010): „Herr de Maizière und sein Radiergummi-Bundesinnenminister will Grundlagen der Internetpolitik neu ordnen“, In: Deutschlandradio:
<http://www.dradio.de/dlf/sendungen/computer/1211701/>
Abgerufen am 03.08.2010

Spiegel Online (2006): Terror-Gefahr. Schäuble erwartet Anschlag mit schmutziger Bombe:
<http://spiegel.de/politik/deutschland/0,1518,397686,00.html>
Abgerufen am 03.05.2010

Tagesspiegel, der (2007): Daten-Skandal weitet sich aus, Verlag Der Tagesspiegel GmbH, Berlin:
<http://www.tagesspiegel.de/politik/international/daten-skandal-weitet-sich-aus/1105400.html>
Abgerufen am 03.05.2010

Webermann, Jürgen (2010): Datenskandal bei der Hamburger Sparkasse?, NDR, Hamburg:
<http://www.ndr.de/wirtschaft/kontodaten100.html>
Abgerufen am 1.08.2010

Wolchon, Marcus (2004): Konzeption und Implementation eines Authentifizierungssystems auf Basis von biometrischen Merkmalen und Transpondertechnologie, GRIN Verlag, München

Zetter, Kim (2010): Airport Scanners Can Store, Transmit Images, wired-magazine, San Francisco:
<http://www.wired.com/threatlevel/2010/01/airport-scanners/>
Abgerufen am 12.5.2010

Ziegler, Michael: Europas (2003): Größte Gesichtserkennungsanlage im Zoo Hannover, Heise, Ct 9/2003, Hannover