

Terrorbekämpfung und Datenschutz:  
**Gräbt die EU ihr eigenes Grab?**

14. Juli 2008

David Raison  
Matrikelnummer: 0316053  
Studienkennzahl: C300  
<david.raison@student.uibk.ac.at>

**Seminararbeit, eingereicht zum Seminar „Terrorismusbekämpfung in der EU“ im Sommersemester 2007 (402060) von Prof. Dr. Heinrich Neisser**

---

## Inhaltsverzeichnis

<b>1</b>	<b>Sicherheit und Überwachung</b>	<b>5</b>
<b>2</b>	<b>Grundrechte und Datenschutz</b>	<b>6</b>
<b>3</b>	<b>Terrorbekämpfung in der EU</b>	<b>7</b>
3.1	Biometrischer Reisepass (Verordnung Nr. 2252/2004) . . . . .	8
3.2	Vorratsdatenspeicherung (Richtlinie 2006/24/EG) . . . . .	9
3.3	Cybercrime Convention (ETS 185) . . . . .	11
<b>4</b>	<b>Die Umsetzungen in Deutschland</b>	<b>13</b>
4.1	Der biometrische Reisepass . . . . .	13
4.1.1	Details zur Umsetzung . . . . .	13
4.1.2	Politische Versprechen und die Rasterfahndung . . . . .	14
4.1.3	Sicherheitsrisiko statt Sicherheitmaßnahme? . . . . .	15
4.1.4	Was taugt der biometrische Pass? . . . . .	16
4.2	Die Vorratsdatenspeicherung . . . . .	17
4.2.1	Details zur Umsetzung . . . . .	17
4.2.2	Was bringt die Vorratsdatenspeicherung? . . . . .	17
4.2.3	Verhältnismäßig und gerechtfertigt? . . . . .	18
4.3	Der „Bundestrojaner“ . . . . .	19
4.3.1	Wozu Online-Durchsuchung? . . . . .	19
4.3.2	Fehlende rechtliche Grundlagen . . . . .	19
4.3.3	Schwierigkeiten bei der Umsetzung . . . . .	21
4.3.4	Schutz der Privatsphäre . . . . .	22
<b>5</b>	<b>Exkurs Österreich</b>	<b>23</b>
<b>6</b>	<b>Gesellschaftliche Auswirkungen</b>	<b>23</b>
6.1	Ende der Unschuldsvermutung? . . . . .	23
6.2	Vertrauensverhältnisse in Gefahr . . . . .	25
6.3	Drang zur Konformität . . . . .	26
6.4	Unzureichender Schutz vor Missbrauch . . . . .	26
<b>7</b>	<b>Verhältnismäßig effektiv?</b>	<b>28</b>
	<b>Literatur</b>	<b>28</b>

## Einleitung

**WAR IS PEACE  
FREEDOM IS SLAVERY  
IGNORANCE IS STRENGTH**

George Orwell: 1984

Die Anschläge des 11. September 2001 und die darauffolgenden Terrorattacken in Madrid und London<sup>1</sup> haben die Bevölkerungen der ins Visier genommenen, westlichen Welt in Angst und Schrecken versetzt. Dieser Schrecken rührte nicht nur daher, weil eine viel zu hohe Zahl an Menschen ihr Leben lassen mussten, sondern auch aus der plötzlichen Erkenntnis, dass Terroranschläge eines solchen Ausmaßes aus heiterem Himmel in den hochtechnologisierten westlichen Nationen überhaupt möglich sind. Um solche verheerenden Attentate in Zukunft rechtzeitig zu vereiteln, haben die betroffenen Staaten und auch die Europäische Union (EU) präventive Maßnahmen beschlossen, neue Sicherheitsbestimmungen erlassen und somit den Exekutiv- und Justizgewalten ein beträchtliches Mehr an Macht in die Hände gelegt.

Die sich vor allem auf den informationstechnologischen Bereich beziehenden Verordnungen und Richtlinien der EU, wie die Richtlinie über die verdachtsunabhängige Vorratsdatenspeicherung<sup>2</sup>, die Verordnung betreffend biometrische Reisepässe<sup>3</sup> oder die im Europarat beschlossene CYBERCRIME CONVENTION (ETS 185), werden daher den Ausgangspunkt dessen darstellen, womit wir uns im Zuge der vorliegenden Arbeit näher beschäftigen werden. Ihrer rechtlichen Natur entsprechend, sind aus diesen Rechtsdokumenten zahlreiche nationale Umsetzungen hervorgegangen, mit dem Ziel, Attentate wie die obigen schon im Keim zu ersticken, also bereits vor ihrer Umsetzung in die Tat zu vereiteln. Dass diese Vorgaben der EU, aber auch des Europarates, vor allem auf informationstechnische Systeme und Netzwerke abzielen, hängt vor allen Dingen damit zusammen, dass auch die vorgeblichen Attentäter bei der Planung ihrer Anschläge zunehmend auf die neuesten Technologien ausweichen. Um mit dieser Entwicklung Schritt halten zu können, so die verantwortlichen Politiker und Leiter von Sicherheitsbehörden, müsse man Rechtsbasen schaffen, die den ermittelnden Behörden die dringend benötigten Instrumente zur Verfügung stellen. Notwendig seien also unter anderem die Möglichkeiten des rückwirkenden Zugriffs auf Computerdateien, Telefongespräche, aber auch auf elektronischen Schriftverkehr.

Dass diese Methoden empfindliche Eingriffe in die Privatsphäre von rund 450 Millionen EU-Bürger und darüber hinaus auch Nicht-EU-Bürgern, ja sogar Beeinträchtigungen der Grundrechte darstellen, ist bekannt. Doch in den Augen der Befürworter sind diese Einbußen an Freiheit das weitaus kleinere Übel, das in Kauf zu nehmen sich überaus lohnt, weil es vermeintlich Sicherheit garantiert. Nichtsdestotrotz fühlen mehr und mehr Menschen sich beobachtet, belauscht und stark in ihren Freiheiten eingeschränkt, und das, obwohl sie weder Hintermänner noch Opfer eines Terroranschlags waren oder sind.

Die mediale Berichterstattung rund um diese Themen, deren Schnittmengen sich grob mit den Begriffen *Datenschutz, Freiheit vs. Sicherheit, Überwachung* und *Informationstechnologien* beschreiben lassen, überschlägt sich tagtäglich. Es vergeht kaum ein Tag, an dem nicht mindesten ein oder zwei Artikel in einschlägigen Medien, aber auch in allgemeinen Tageszeitungen zur unüberschaubaren Fülle an Informationen zu diesen Themen beitragen.

In dieser Arbeit soll demnach der Frage nachgegangen werden, ob die EU und ihre Mitgliedsstaaten sich in ihrem Überwachungswahn letztendlich nicht mehr schaden als dass diese Maßnahmen zu Abwendung von Terroranschlägen dienen. Inwiefern schränkt die EU die Freiheit ihrer Bürger, und nicht nur die potentieller Attentäter ein? Büßt sie damit nicht letztlich eines ihrer primären Definitionsmerkmale, ein demokratisch-liberaler Zusammenschluss zu sein ein? Eine diese Arbeit durchziehende Frage wird also sein, ob die EU, in ihren Bestrebungen zu mehr Sicherheit, nicht vielleicht selbst zu einer intoleranten, restriktiven und starren Gesellschaft

---

<sup>1</sup>Madrid: 11 März 2004; London: 7. Juli 2005

<sup>2</sup>Richtlinie 2006/24/EG

<sup>3</sup>Verordnung 2252/2004

wird? Etwas provokanter formuliert: *Wie weit entfernt wäre ein solches Gebilde von der Horrorvorstellung einer rückwärtsgewandten, eingeschüchterten und unmündigen Gesellschaft, vor deren Etablierung durch den islamistischen Terror man sich ursprünglich schützen wollte?*

Um diesen Fragen nachgehen zu können, werden wir uns zunächst dem Verhältnis von Überwachung und Sicherheit widmen müssen. (1) Führt mehr Überwachung automatisch und unbedingt zu mehr Sicherheit? Und falls ja, zu welchem Preis? (vgl. Peissl, 2002, S. 7)

Es sollte allerdings schon zu Beginn klar gemacht werden, dass die vorliegende Arbeit nicht den Anspruch erheben kann, das gesamte mit dieser Problematik verbundene Umfeld zu untersuchen; wenngleich es dem Autor auch nicht leichtgefallen ist, aus der bereits zuvor erwähnten Flut an Informationen und dem breiten Spektrum an verwandten Themen eine pointierte Auswahl zu erstellen. Es sind daher zunächst ein paar grundlegende Einschränkungen notwendig, um das Profil zu schärfen. So muss unter anderem auf eine Betrachtung der soziologischen Grundbedingungen, welche solch intensive Eingriffe in die persönlichen Grundrechte erst ohne vehementeste Widerstände der Bürger ermöglichen<sup>4</sup>, verzichtet werden.

Im Gegenzug dazu und zur Beantwortung der eben aufgestellten Fragen, soll aber sehr wohl auf die gesellschaftlichen Konsequenzen eingegangen werden, die aus dem aktuellen „Überwachungswahn“ resultieren können und im Extremfall auch werden. Dem gegenüber können, diesen gesamten Bereich umfassende, datenschutzrechtliche Aspekte jedoch nur am Rande besprochen werden<sup>5</sup>, obwohl es nicht zuletzt Ziel und Aufgabe des Datenschutzes ist, Eingriffen in die Privatsphäre, wie den oben beschriebenen, Grenzen zu setzen. Die Diskussion müsste sich dann allerdings auch auf die Reformen ausweiten, deren die wenigen auf EU-Ebene bestehenden datenschutzrechtlichen Bestimmungen bedürfen. Allein diese spezifische Thematik würde mitunter jedoch eine eigene Arbeit rechtfertigen und inhaltlich ausfüllen.

Folglich werden wir uns, wie bereits erwähnt, zunächst ab Seite 5 mit der Frage befassen, in welcher Relation Überwachung und Sicherheit stehen, um dann im zweiten Kapitel die Grund-, Freiheits- und Datenschutzrechte zu beleuchten, die von den beschlossenen Sicherheitsmaßnahmen potentiell verletzt werden. Das so erworbene Vorwissen wird unabdingbar sein, um in der Folge untersuchen zu können, wie die im dritten Kapitel ab Seite 7 beschriebenen Dokumente der EU und des Europarats Terrorgefahren abwehren und Sicherheit gewährleisten sollen. In jenem Kapitel werden wir versuchen eine Übersicht über drei spezifische Dokumente, nämlich (3.1) die Verordnung der EU über einen biometrischen Reisepass, (3.2) die Richtlinie über eine verdachtsunabhängige Vorratsspeicherung von Daten sowie die vom Europarat und 6 weiteren Staaten beschlossene (3.3) Cybercrime Konvention, zu vermitteln.

Im Kapitel 4 ab Seite 13 soll anhand der Bundesrepublik Deutschland exemplarisch auf die Probleme, Schwierigkeiten und Gefahren hingewiesen werden, die sich durch die Umsetzungen der EU-Vorgaben ergeben haben und noch ergeben könnten. Dabei wurde sich erneut auf drei konkrete Beispiele beschränkt<sup>6</sup>, die sich rechtlich jeweils auf eine der Vorgaben stützen. Im Anschluss an diese Veranschaulichungen soll uns im Kapitel 5 auf Seite 23 ein Exkurs auf die Situation in Österreich jedoch nicht verwehrt bleiben.

Schließlich werden wir in Kapitel 6 auf Seite 23 darauf eingehen, welche gesellschaftlichen Auswirkungen die vermeintlichen Sicherheitsbestrebungen haben werden. Die Fragen, wie sich der staatliche Schutz vor Terrorbedrohungen auf die Unschuldsvermutung, Vertrauensverhältnisse und ganz allgemein auf liberale Gesellschaften

<sup>4</sup>Dazu gehören z.B. Fragen wie: „Ergeben wir uns statt einer Hinschau- zunehmend einer Wegschau-Mentalität?“, „Braucht es mehr Überwachung, weil die soziale Kontrolle abnimmt?“ oder „Welchen Einfluß auf diese Entwicklungen haben Individualisierung, Technik und Medien, besonders das Internet?“ Der Hamburger Datenschutzbeauftragte Hartmut Lubomierski stellt in dieser Hinsicht fest, dass „[a]us der Horrorvision einer totalen Überwachung der Menschen [...] heute weitgehend die Vorstellung geworden [ist DR], durch den Einsatz von Technik und Datenerfassung würden sowohl unsere individuelle als auch unsere gesamtgesellschaftliche Sicherheit erhöht und unsere Kommunikations- und Informationsbedürfnisse besser und bequemer befriedigt.“ Lubomierski (2006, S. 2)

<sup>5</sup>Dies werden wir im Kapitel 2 auf Seite 6 tun.

<sup>6</sup>Leider nicht beachtet werden können weitere Umsetzungen und „Anwendungen“, wie z.B. die Verbindung von Videoüberwachung und Oyster-Card in Großbritannien, elektronische Gesundheitsakten, Austausch von Fluggastdaten, die Verwendung von Mautdaten und die automatische KFZ-Zeichen Erkennung zum Zwecke der Verbrechensaufklärung, die sogenannte Anti-Terror-Datei, die rezenten Abhörgesetze in Schweden, die DNA-Analyse, EMD (Electro-Muscular-Disruption) Safety Bracelets (euphemistisch als Electronic ID Bracelets bezeichnet) u.v.m.

auswirken wird, wird uns schlussendlich zur Betrachtung der Effektivität und Verhältnismäßigkeit der Europäischen Terrorbekämpfung auf Seite 28 führen.

Neben den Primärquellen in Form der Dokumente der EU und des Europarats sind in die vorliegende Arbeit hauptsächlich Informationen aus Beiträgen einschlägiger deutschsprachiger Magazine und Online-Zeitschriften aus dem informationstechnischen Bereich eingeflossen. Da sich die Berichterstattung schwerpunktmäßig auf die Bundesrepublik konzentrierte und der größte Widerstand gegen diese Umsetzungen auch aus der BRD zu kommen scheint, bot es sich an, Deutschland als Beispiel für die Umsetzungen her zu nehmen.

## 1 Sicherheit und Überwachung

*„Der Ruf nach mehr Sicherheit wird fälschlicherweise oft mit dem Ruf nach verstärkter Überwachung gleichgesetzt.“* (Peissl, 2001, S. 1)

Bevor man sich mit den Terrorbekämpfungsmaßnahmen eines Staates oder, in unserem Fall, der EU beschäftigt, sollte klar sein, was diese Vorkehrungen eigentlich zu schützen suchen. Welche Eigenschaften und Errungenschaften eines Staates, welche Rechte der StaatsbürgerInnen<sup>7</sup> sollen vor Terror gesichert werden?. Ohne großes Zögern sollten an dieser Stelle Begriffe wie *Menschenrechte*<sup>8</sup>, *Freiheit* und *Demokratie* fallen. Und dennoch ist das Verhältnis dieser Eigenschaften zu ihrer Sicherung oft ein prekäres. Das als „*Demokratie-Dilemma*“ bekannte Problem der Verhältnisse von Sicherheit und Freiheit sowie Sicherheit und Überwachung zeigt sich eben auch darin, inwiefern die eingesetzten Mittel demokratische Werte eher einschränken und verletzen, als dass sie diese schützen würden. (vgl. Ganor, 2006, S. 178) Insofern besteht eine elementare Schwierigkeit beim Abwägen von Zielen und Mitteln der Terrorbekämpfung darin, mit den angestrebten Abwehrmaßnahmen nicht selbst die Ziele der Terroristen, nämlich „demokratische Gesellschaften zu destabilisieren bzw. deren Werte anzugreifen“ (Peissl, 2001, S. 2) zu verwirklichen.

Der Grad, der darüber entscheidet, ob Sicherheit der Freiheit dienlich ist, oder sie eher einschränkt, ist sehr schmal. Ob und inwiefern diese Linie bei den im übernächsten Kapitel behandelten Texten und deren nationalen Umsetzungen in der BRD überschritten wurde, wird im weiteren Verlauf dieser Arbeit noch zu klären sein. Auf die Frage, ob die Menschenrechte zur Bekämpfung des Terrorismus notgedrungen eingeschränkt werden müssen, hat die INTERNATIONAL COMMISSION OF JURISTS in ihrer BERLIN DECLARATION ON UPHOLDING HUMAN RIGHTS AND THE RULE OF LAW IN COMBATING TERRORISM bereits eine Antwort gegeben. Der Deklaration zu Folge, bieten die derzeit gültigen Menschenrechte den Staaten einen ausreichend großen Spielraum bei der Bekämpfung des Terrorismus, ohne dass die Rechte verletzt werden müssten. (vgl. Conte, 2006, S. 291) Dennoch wird gerne und häufig darauf hingewiesen, dass die vormals so hoch geschätzten Rechte, wie u.a. das Recht auf informationelle Selbstbestimmung<sup>9</sup>, im Hinblick auf die Sicherheit der Allgemeinheit einen neuen, verringerten Stellenwert einnehmen werden. (Kwiatkowski *et al.*, 2006, S. 244)

Der Europäische Gerichtshof (EuGH) hat bereits 1978 in seiner Entscheidung zum Fall *Klass u.a.* gegen Deutschland auf dieses sensible Verhältnis hingewiesen:

*„[...] Staaten dürfen nicht im Namen des Kampfes gegen Spionage und Terrorismus alle Maßnahmen ergreifen, die sie (sic) geeignet halten [...] die Gefahr (besteht darin), die Demokratie, die verteidigt werden soll, zu untergraben oder gar zu zerstören“* (zit. n. Neisser, 2006)

---

<sup>7</sup>Hier sind ebenso EU-BürgerInnen gemeint, wenngleich dem Autor durchaus bewusst ist, dass die EU kein Staat im eigentlichen Sinne, sondern ein Gebilde „*sui generis*“ ist.

<sup>8</sup>Auf die in diesem Kontext relevanten Rechte und die entsprechenden Gesetzestexte werden wir noch im nächsten Kapitel eingehen.

<sup>9</sup>Das Recht auf informationelle Selbstbestimmung besagt, dass jeder Mensch selbst entscheiden können soll, wem er seine persönlichen Daten wann, zu welchen Zwecken zugänglich macht.

Manche Sicherheitspolitiker gehen demnach uneingeschränkt davon aus, dass mehr Überwachung auch mehr Sicherheit bedeutet. Hans-Peter Uhl ist laut eigener Aussage davon überzeugt, dass man mit „möglichst vielen Daten und Datenabgleich [...] Sicherheit produzieren kann.“ (zit. n. Krempl & Kuri, 2006d) Doch diese Überzeugung ist in mehrfacher Hinsicht problematisch. Denn die so produzierte Sicherheit ist nämlich, ebenso wie die Terrorbedrohung selbst nur eine gefühlte Bedrohung ist<sup>10</sup>, auch nur eine gefühlte Sicherheit. Überwachung kann niemanden effektiv davor schützen Opfer eines Terroranschlags zu werden, vor allem dann nicht, wenn es sich um bisher unbekannte, religiös motivierte Selbstmordattentäter handelt, die z.B. *vor* Überwachungskameras nicht zurückschrecken und *von* ihnen auch nicht enttarnt werden können.

Eines der Prinzipien, die bisher in Rechtsstaaten dafür gesorgt haben, dass die Freiheit der Bürger mit ihrer staatlich garantierten Sicherheit einhergeht, wird derzeit aufgeweicht. Die Trennung von strafverfolgender Polizei und präventiv ermittelnden Geheimdiensten, die in Deutschland sogar verfassungsrechtlich verankert ist, soll vermeiden, dass eine Geheimpolizei wie die Gestapo nie wieder möglich ist. Doch deutsche Politiker wie Wolfgang Schäuble sind darauf erpicht, die Datenbanken von Polizei und Nachrichtendiensten in einer sog. „Islamistendatei“ zusammen zu legen. (vgl. Lambrecht, 2005)

Wenn man also die angewandten Sicherheitsvorkehrungen als strukturelle Gewalt des Staates gegenüber seinen Bürgern ansieht, dann wird einem bewußt, dass der Staat, „[u]m die Gewalt des Einzelnen zu bekämpfen, [...] selbst Gewalt [ausübt].“ (Trojanow, 2008) Je mehr Macht den Behörden zugesprochen wird, desto chancenloser wird in der Tat der Verbrecher, doch „die Kriminalität [wäre] keineswegs abgeschafft, sondern vom Individuum auf den Staat verlagert“ (Trojanow, 2008)

Das Verhältnis zwischen Überwachung, Sicherheit und einer freien, lebenswürdigen Gesellschaft ist durchaus ein sehr schwieriges, und die Zusammenhänge nicht immer auf den ersten Blick erkennbar. Nicht ganz zufällig erinnert diese Situation an George Orwells Dystopie 1984. So zitiert Trojanow in seinem Text den Müncher Polizeipräsidenten Wilhelm Schmidbauer mit den Worten: „Wer Videoüberwachung und die polizeiliche Erhebung von Telefonverbindungsdaten infrage stellt, macht unsere Gesellschaft ein Stück weit unmenschlicher.“ (zit. n. Trojanow, 2008) und schlussfolgert daraus, dass demzufolge wohl „der absolute Überwachungsstaat der menschlichste aller möglichen Staaten und Orwells 1984 eine positive Utopie“ (Trojanow, 2008) sei.

Benjamin Franklin soll einmal gesagt haben:

*„Diejenigen, die ihre Freiheit zugunsten der Sicherheit aufgeben, werden am Ende keines von beiden haben – und verdienen es auch nicht.“* (zit. n. Krempl & Kuri, 2006b)

## 2 Grundrechte und Datenschutz

Um die Frage beantworten zu können, ob die Maßnahmen der EU und ihrer Mitgliedstaaten die Grundrechte ihrer Bürger (unverhältnismäßig) beschneiden, muss man zunächst wissen, auf welche Rechte man als Bürger der EU überhaupt Anspruch hat. Entsprechend unserer Thematik, und wie bereits zuvor angekündigt, wird an dieser Stelle lediglich kurz auf die elementaren, vor allem im Zusammenhang mit elektronischer Datenverarbeitung bestehenden Rechte und Gesetzestext eingegangen. Neben der Datenschutzrichtlinie (95/46/EG) und der Datenschutzrichtlinie für die elektronische Kommunikation (2002/58/EG)<sup>11</sup>, auch „E-Privacy-Richtlinie“ genannt, existieren eine Reihe grundlegenderer Rechtstexte, auf die sich die beiden EU-Richtlinien auch jeweils beziehen. Wenn auch der Bezug dieser Grundrechte zu den in der Folge zu behandelnden Terrorismusbekämpfungsmaßnahmen an dieser Stelle noch nicht ersichtlich sein mag, so wird dieser allerspätestens bei der näheren Betrachtung der Deutschen Umsetzungen in Kapitel 4 klar werden.

<sup>10</sup>Laut Ilija Trojanow ist die Gefahr, Opfer eines Terroranschlags zu werden, ebenso gering wie die Chancen, beim Lotto zu gewinnen. vgl. Trojanow, 2008

<sup>11</sup>Ein Reformentwurf zu dieser Richtlinie wird derzeit im Europäischen Parlament debattiert.

Artikel 8 der, durch Artikel 6 EUV für alle EU-Mitgliedstaaten geltenden, Europäischen Menschenrechtskonvention (EMRK) bezeichnet bereits das „Recht auf Achtung des Privat- und Familienlebens“, das sich ebenso auf Wohnung und Korrespondenz ausdehnt<sup>12</sup>. Der zweite Absatz des Artikels definiert gleichermaßen, in welchen exklusiven, jedoch m.E. ziemlich breit und offen formulierten Fällen dieses Recht eingeschränkt werden darf:

*„Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.“*

Neben der EMRK regelt besonders die Datenschutzkonvention 108 des Europarates aus dem Jahr 1981 die Rechte eines europäischen Staatsbürgers in Bezug auf Datensammlung und -Verarbeitung. Der als „Golden Rule des Datenschutzes“ bekannte Artikel 8 dieser Konvention gesteht jedem Betroffenen das Recht auf Auskunft über ihn betreffende Datensammlungen und deren Inhalt zu. Allerdings wird dieses Recht in Artikel 9 relativiert: Das Recht auf Auskunft kann nämlich bei Gefährdung der Staats- oder der öffentlichen Sicherheit verweigert werden, aber auch, wenn dies zum Zweck der Verfolgung von Straftaten von Nöten ist. (vgl. Gamper, 2007, S. 28) Dieser in Artikel 9 der Konvention 108 skizzierte Grundsatz wird sich in der Folge an den jeweiligen Umsetzungen der Mitgliedsstaaten der EU und des Europarates messen müssen.

Die Richtlinie 95/46/EG übernimmt, wie bereits zuvor erwähnt, nicht nur dieses Auskunftsrecht in Artikel 12, sondern erweitert ebenso die zulässigen Ausnahmen in Artikel 13: Sollte dies im Rahmen der Landesverteidigung oder bei wichtigen wirtschaftlichen oder finanziellen Interessen eines Mitgliedstaates oder der EU als notwendig erachtet werden, kann die Auskunft verweigert werden. Verweigert werden kann die Auskunft weiterhin, wenn dies zum Schutz des Betroffenen oder der Freiheiten anderer Personen passiert. (vgl. Böckle, 2004, S. 45f)

Die E-Privacy-Richtlinie übernimmt diese Ausnahmen in Artikel 15 Absatz 1 ebenfalls, allerdings mit der Beschränkung, dass es sich nicht um eine allgemeine oder erkundende Überwachung handeln darf. (vgl. Böckle, 2004, S. 69f)

### 3 Terrorbekämpfung in der EU

Die Europäische Gesetzgebung zur Terrorismusbekämpfung ist allein deswegen schon schwer zu fassen, weil sich einerseits die Verordnungen, Richtlinien und Zuständigkeitsbereiche auf die verschiedenen Säulen der EU aufteilen und andererseits auch Konventionen des Europarats zu berücksichtigen sind. Die Gesetzgebung der Europäischen Union ist allerdings verzwickelt und teilweise umstritten. So wurde die unter Punkt 3.2 behandelte Richtlinie zur Vorratsspeicherung in der ersten Säule als Harmonisierungsinstrument angesiedelt, obwohl sie Maßnahmen beschreibt, die eigentlich in die dritte Säule, die Polizeiliche und Justizielle Zusammenarbeit in Strafsachen (PJZS) gehören. Auf diese Problematik und ihre Folgen werden wir jedoch später noch genauer eingehen. Zu beachten ist in diesem Zusammenhang ausserdem, dass sich die EU-Rechtsakte zum Datenschutz auf die 1. Säule beschränken, weshalb die Kommission Defizite im Bereich der PJZS eingesteht<sup>13</sup>. (vgl. Gamper, 2007, S.31)

<sup>12</sup>Auf die heutige Zeit umgelegt, beinhaltet dieses Recht nach allgemeiner Auffassung auch den Schutz von Verkehrs- und Zugangsdaten zu elektronischen Kommunikationsnetzen. Larnhof (vgl. 2006, S. 63)

<sup>13</sup>Am 4. Oktober 2005 hat die Kommission aus diesem Grund dem Rat einen „Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.“ vorgelegt. Doch wie bereits Eingangs erwähnt, würde eine eingehendere Befassung mit den Datenschutz auf EU-Ebene den Rahmen der vorliegenden Arbeit sprengen.

Neben den Abkommen auf EU Ebene sind wie zuvor angedeutet aber auch Nicht-EU Abkommen zu beachten. So ist neben der noch näher zu beleuchtenden CYBERCRIME-CONVENTION des Europarates zum Beispiel ebenfalls der VERTRAG ÜBER DIE VERTIEFUNG DER GRENZÜBERSCHREITENDEN ZUSAMMENARBEIT, INSBESONDERE ZUR BEKÄMPFUNG DES TERRORISMUS, DER GRENZÜBERSCHREITENDEN KRIMINALITÄT UND DER ILLEGALEN MIGRATION<sup>14</sup> von Bedeutung. Die Bestimmungen dieses Vertrags, der seit dem 13. Juni 2007 zum Teil in die 3. Säule der EU überführt wurde, erlauben Strafverfolgern in den Mitgliedstaaten ihre Daten zu Fingerabdrücken, aber auch genetischen Informationen oder Kraftfahrzeugen *automatisiert* auszutauschen. (vgl. Krempl, 2007e)

### 3.1 Biometrischer Reisepass (Verordnung Nr. 2252/2004)

Die Verordnung, deren vollständige Bezeichnung VERORDNUNG NR 2252/2004 DES RATES VOM 13. DEZEMBER 2004 ÜBER NORMEN FÜR SICHERHEITSMERKMALE UND BIOMETRISCHE DATEN IN VON DEN MITGLIEDSTAATEN AUSGESTELLTEN PÄSSEN UND REISEDOKUMENTEN lautet, wurde aus den folgenden, in ihrer Preamble angegebenen Gründen erlassen:

Zunächst (Grund 2) sollen die Sicherheitsstandards der Reisedokumente erhöht werden, um einen besseren Schutz vor Fälschungen zu gewährleisten. Zu diesen Sicherheitsstandards gehören somit ebenfalls biometrische Merkmale wie das Gesichtsbild und die Fingerabdrücke des Inhabers. Diese Indikatoren sollen ermöglichen, dass die Verbindung des Dokuments mit seinem rechtmässigen Besitzer zweifelsfrei sichergestellt werden kann. Weiters sollen die Pässe, die, wie in Grund 3 angegeben, den Standards<sup>15</sup> der Internationalen Zivilluftfahrt-Organisation (ICAO) zu entsprechen haben, eine „betrügerische Verwendung“ der Dokumente ausschließen.

Die Verordnung regelt jedoch bewusst nicht (Grund 4), wer auf die Daten zugreifen darf. Welchen Behörden der Zugriff auf die auf den Pässen gespeicherten Daten gestattet sein soll, liegt demnach im Ermessen der nationalen Gesetzgeber. Die Verordnung verweist zum Zwecke des Datenschutzes in Grund 8 auf die Bestimmungen der Datenschutzrichtlinie 95/46/EG und sieht, in Grund 9, das in Artikel 5 Absatz 3 EGV definierte Prinzip der Verhältnismässigkeit als gegeben.

Inhaltlich ist die Verordnung zunächst wenig spektakulär. Die nachfolgenden Artikel werden aber im Hinblick auf ihre nationalstaatlichen Umsetzungen von Relevanz sein.

**Artikel 1**, der darauf hinweist, dass es sich bei den folgenden Merkmalen um Mindestnormen handelt, besagt ebenfalls, dass sich das Gesichtsbild sowie die Fingerabdrücke in einem gesicherten Format auf dem Speichermedium des Reisedokuments zu befinden haben. Das Speichermedium müsse dabei geeignet sein, die Integrität, Authentizität und die Vertraulichkeit der Daten sicher zu stellen.

**Artikel 4 Absatz 1** spricht den Inhabern eines solchen Passes „das Recht [zu], die personenbezogenen Daten in dem Pass oder dem Reisedokument zu überprüfen und gegebenenfalls eine Berichtigung oder Löschung zu beantragen.“

**Artikel 4 Absatz 3** erklärt darüber hinaus, dass die erhobenen biometrischen Daten nur dazu verwendet werden dürfen, die Authentizität des Dokumentes zu überprüfen sowie die Identität des Inhabers zu überprüfen. (sic!) Dies allerdings auch nur dann, wenn die Vorlage eines Passes gesetzlich vorgeschrieben ist.

---

<sup>14</sup>Dieser Vertrag wird unter anderem auch als VERTRAG VON PRÜM oder SCHENGEN-III-VERTRAG bezeichnet.

<sup>15</sup>Diese Standards sind im ICAO Dokument 9303 angegeben.

### 3.2 Vorratsdatenspeicherung (Richtlinie 2006/24/EG)

Die Richtlinie 2006/24/EG, die bereits im Dezember 2005 von Europäischem Parlament (EUP) beschlossen wurde, heißt in ihrer ganzen Pracht RICHTLINIE 2006/24/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES VOM 15. MÄRZ 2006 ÜBER DIE VORRATSSPEICHERUNG VON DATEN, DIE BEI DER BEREITSTELLUNG ÖFFENTLICH ZUGÄNGLICHER ELEKTRONISCHER KOMMUNIKATIONSDIENSTE ODER ÖFFENTLICHER KOMMUNIKATIONSNETZE ERZEUGT ODER VERARBEITET WERDEN, UND ZUR ÄNDERUNG DER RICHTLINIE 2002/58/EG

Die Richtlinie, die eigentlich Instrumente zur Strafverfolgung fordert und sich somit ungewöhnlicherweise mit Begebenheiten der 3. Säule der EU befasst, konnte nur deshalb von der Kommission ausgearbeitet und im Harmonisierungsbereich angesiedelt werden, da verschiedene Mitgliedsländer bereits Gesetze zur Vorratsdatenspeicherung erlassen hatten. Die so gespeicherten Daten konnten, nach Argumentation der Kommission jedoch nicht effizient verwendet werden, so dass ein Harmonisierungsbedarf bestand. In einem Positionspapier der INTERNET SERVICE PROVIDERS ASSOCIATION (ISPA) wird dagegen allerdings argumentiert, dass dieser Bedarf nie bestanden hätte, da bis dahin in keinem Land eine verpflichtende Vorratsdatenspeicherung praktiziert wurde. (vgl. Larnhof, 2006, S. 47) Auch nach der Regelung scheint das Ziel der Harmonisierung nicht vollends erreicht worden zu sein. Dies geht aus den Aussagen Klaus Landefelds vom Verband der deutschen Internetwirtschaft eco hervor. Aus der Sicht der Internetprovider sei der Harmonisierungsansatz der Kommission durch die unterschiedlichen Umsetzungsgesetze integral verloren gegangen. Die Vorkehrungen, was wie lange zu speichern ist, seien einfach zu divers. (Kreml & Kuri, 2007a)

Nicht nur dieser Meinung, sondern auch der Meinung, dass es sich um eine Angelegenheit der Strafverfolgung handle, es also eines Rahmenbeschlusses des Rats bedurft hätte und es sich bei der vorliegenden Richtlinie um eine Kompetenzüberschreitung der EU-Kommission handle, sind hingegen die Staaten Slowenien und Irland. Beide Mitgliedstaaten stimmten nicht nur im Ministerrat gegen die Richtlinie, sondern reichten auch beim EuGH Klage gegen die Richtlinie ein. (vgl. Larnhof, 2006, S. 46)

Zu Gunsten der Kommission muss allerdings gesagt werden, dass man sich über einen zuvor von Irland, Schweden, Frankreich und Großbritannien vorgelegten Entwurf zu einem Rahmenbeschluss nie hatte einigen können. Der im April 2004 vorgelegte Rahmenbeschluss<sup>16</sup> sah eine 12 bis 36-monatige Aufbewahrung der Verkehrs- und Rufdaten vor und war dabei auch nicht auf schwere Straftaten und Terrorismusbekämpfung beschränkt. (vgl. Larnhof, 2006, S. 45) Irland und Slowenien möchten aber nicht die Vorratsdatenspeicherung an sich in Frage stellen<sup>17</sup> sondern lediglich die Zuständigkeitsfragen bei der EU-Gesetzgebung. (vgl. Kreml & Kuri, 2006a) Wenngleich am ersten Juli 2008 ein Hearing des Falles C-301/60 am EuGH in Luxemburg stattfand, wird mit einem Resultat nicht vor 2009 gerechnet. (fut, 2008)

Die Richtlinie regelt in ihrer jetzigen Form die Speicherung von Ruf- und Verkehrsdaten für eine Dauer von mindestens 6 und höchstens 24 Monaten. Wie lange die Daten in diesem Rahmen nun genau gespeichert werden sollen, wurde hingegen den Mitgliedstaaten überlassen. (vgl. Larnhof, 2006, S. 3) Ebenfalls den nationalen Umsetzungen überlassen blieben Bestimmungen, in welcher Form der Zugriff auf die Daten zu beschränken und welche Behörden überhaupt Zugriff haben dürfen. In der Verantwortung der Mitgliedstaaten verblieb auch, eine oder mehrere unabhängige Kontrollstellen mit der Überprüfung der Datenspeicherung zu beauftragen. (vgl. Larnhof, 2006, S. 51ff)

Da die Richtlinie recht vage formuliert ist und ziemlich viele Aspekte offen lässt, darf bezweifelt werden, dass sie den Anspruch der Harmonisierung erfüllt. So ist in der Richtlinie unter Anderem nicht angegeben, welche Verbrechen mit dem Ausdruck „schwere Verbrechen“ gemeint sind oder wo die Daten überhaupt zu speichern seien. Einige Staaten, darunter Deutschland, haben sich daher für eine dezentrale Speicherung der Daten bei den Dienstleistern, bei denen sie anfallen, entschieden. Andere Mitgliedstaaten, wie z.B. Österreich, wollen die

<sup>16</sup>Ratsdokument 8958/04

<sup>17</sup>Im Januar 2008 hat die irische Regierung das Vorhaben geäußert, den irischen Telekommunikationsanbietern per Verordnung vorzuschreiben, Verbindungs- und Standortdaten für die Dauer von drei Jahren auf Vorrat zu speichern. Kreml & Kuri (vgl. 2008b)

Daten zentral auf Vorrat speichern. (vgl. Larnhof, 2006, S. 56)

Zu den wichtigsten Inhalten der Richtlinie zählen zunächst, zwecks datenschutzrechtlicher Bestimmungen, die Verweise auf die Richtlinien 95/46/EG und 2002/58/EG (Grund 1 bzw. 2). Ebenfalls wird auf den in Kapitel 2 erwähnten Artikel 9 der EMRK verwiesen (Grund 9). Die Vorratsdatenspeicherung, so geht aus der Richtlinie hervor, sei eine notwendige Maßnahme wie nach Artikel 9 EMRK gefordert. Des Weiteren wird auf die Datenschutzkonvention 108 des Europarates verwiesen (Grund 20) und Personen, denen aus einer rechtswidrigen Verarbeitung ihrer Daten Schaden entsteht, wird ein Recht auf Schadensersatz zugestanden. (Grund 19) Es soll zudem verhindert werden, dass die Daten, sofern sie nicht zu Strafverfolgungszwecken abgerufen wurden, nicht mehr als einmal auf Vorrat gespeichert werden (Grund 13).

Wiederum wird auf die Einhaltung des Verhältnismäßigkeitsprinzips (Artikel 5 Absatz 3 EGV) verwiesen (Grund 21), um abschließend in Grund 25 unmissverständlich darauf hinzuweisen, dass die Fragen des Zugangs zu den Vorratsdaten nicht in den Anwendungsbereich des Gemeinschaftsrecht fallen und somit auch nicht in der Richtlinie berührt werden.

Was die Bestimmungen der Richtlinie betrifft, so regeln diese vor allem die Art der zu speichernden Daten:

**Artikel 1 Absatz 2** verweist eindrücklich darauf, dass von natürlichen wie von juristischen Personen Verkehrs- und Standortdaten zu speichern sind, nicht jedoch Inhaltsdaten.

**Artikel 5** beschreibt die zu speichernden Daten. Diese sind zur Veranschaulichung in **ABBILDUNG 1** grafisch dargestellt.

**Artikel 9** fordert die Mitgliedstaaten auf, bei der Umsetzung der Richtlinie eine oder mehrere öffentliche, unabhängige Kontrollstellen mit der Kontrolle der Vorratsdatenspeicherung und der Zugriffe zu beauftragen.

**Artikel 15** schließlich ermöglicht den Mitgliedstaaten, über die Umsetzungsfrist der Richtlinie hinaus die Umsetzung der Vorratsdatenspeicherung von Internet-Verkehrsdaten bis zum 15. März 2009 auszusetzen. Jedoch nur dann, wenn diese Absicht bei Unterzeichnung der Richtlinie bereits erklärt wurde. Im Rahmen der vorliegenden Arbeit ist besonders darauf hinzuweisen, dass u.a. Deutschland eine solche Erklärung abgegeben hat.



- Betrug mit und durch Computernetzwerke,
- Besitz und Verbreitung von Kinderpornografie, aber auch
- Urheberrechtsverstöße. (vgl. Europarat, 2001, S. 4ff)

Die Konvention fordert ihre Unterzeichner dazu auf, Gesetze zu stimmen, die ihren Behörden die Suche in und den Zugang zu sämtlichen Computersystemen und Datenspeichern, die sich auf ihren Territorien befinden, ermöglichen, um so die eben aufgelisteten Tatbestände ermitteln zu können. In Artikel 19 der Konvention wird besonders gefordert, dass, sollte Grund zur Annahme bestehen, dass sich das gesuchte Material auf weiteren Rechnern oder Datenträgern befindet, sich auch auf diese Geräte Zugang verschafft werden können soll. Ermittler sollen ebenfalls dazu berechtigt werden, Computer oder Datenträger zu beschlagnahmen, die Daten zu kopieren und gegebenenfalls sogar auf dem Ursprungsgerät zu löschen oder den Zugriff darauf zu verhindern. (vgl. Europarat, 2001, S. 11f) Besonders diese Bestimmungen werden in der Folge von Relevanz sein, wenn wir uns in Kapitel 4.3 mit dem Instrument der „Online-Durchsuchung“ in der BRD beschäftigen werden.

Die Konvention enthält ausserdem, ähnlich der Richtlinie 2006/24/EG, Bestimmungen zur Speicherung von Computer-, Verkehrs- und Kundendaten<sup>18</sup>. Allerdings ist die Rede hier von Data Preservation, also anlassbezogener anstelle von verdachtsunabhängiger Speicherung. Das Schriftstück enthält ebenso Angaben zur Methode der Offenlegung dieser Daten für Behörden des jeweiligen Staates. (vgl. Europarat, 2001, S. 10) Da die, durch die Vorratsdatenspeicherung erhobenen Daten, auf Anforderung den Ermittlungsbehörden jedes Unterzeichnerstaates zur Verfügung gestellt werden sollen (vgl. Krempel, 2007a, S. 61), regelt die Konvention im Anschluß an die Speicherungsmodalitäten ebenfalls die internationale Zusammenarbeit, speziell den Datenaustausch zwischen den Staaten<sup>19</sup>, aber auch die Auslieferung von Straffälligen. Ein Unterzeichnerstaat soll angeforderte Daten nur dann verweigern können, wenn die Straftat nach seinem Ermessen politischer Natur ist oder wenn die Bereitstellung der Daten die Souveränität, Sicherheit oder öffentliche Ordnung des Staates gefährden könnte. (vgl. Europarat, 2001, S. 19)

Die Konvention bezieht sich jedoch nicht nur auf reine Computerkriminalität, sondern auch auf die Sammlung von Daten über beliebige, strafrechtlich relevanten Aktivitäten. Wegen seiner Drastik besonders hervorzuheben ist die Forderung, den Ermittlungsbehörden das Recht zu geben, Privatpersonen zur Mithilfe beim Zugriff auf, und bei der Entschlüsselung von Daten zu verpflichten. (vgl. Čas, 2001, S. 3) Die Gesetze sollen sich auch nicht ausschließlich auf öffentliche Systeme begrenzen, sondern nach Möglichkeit auch für privat genutzte und isolierte Computernetzwerke gelten. (vgl. Europarat, 2001, S. 9)

Bemängelt wird an der Konvention besonders die unzureichende Berücksichtigung von Datenschutzbestimmungen. Diese Tatsache rührt daher, dass die Vorarbeiten zum Text fast ausschließlich von Polizei und Ermittlungsbehörden durchgeführt wurden. So widerspricht die Konvention in einigen Punkten offenkundig der EMRK und den beiden Datenschutzrichtlinien der EU: sie regelt keine Verpflichtung zum richterlichen Vorbehalt und enthält auch keine Bestimmungen bezüglich der Beschränkung der Nutzung der angehäuften Daten. (vgl. Čas, 2001, S. 3) Im Einklang mit den restlichen Artikeln der Konvention haben auch die Hinweise auf Beachtung der nationalen Datenschutz- und der Menschenrechte nur Vorschlagscharakter, obwohl in der Preamble explizit darauf hingewiesen wird, dass man sich eines Gleichgewichts zwischen den Interessen der Ermittlungsbehörden und den Menschenrechten sehr wohl bewusst sei. Die Meinungsfreiheit, die Freiheit, sich Informationen aller Art zu verschaffen, der Respekt der Privatsphäre, wie auch die Datenschutzkonvention des Europarates habe man sich bei der Erstellung der Konvention vor Augen gehalten. (vgl. Europarat, 2001, S. 2)

<sup>18</sup>Als Kundendaten - „Subscriber information“ im englischen Original - bezeichnet die Konvention eine breite Palette an Informationen, darunter die Art der Verbindung, die Dauer derselben, die Identität des Kunden, einschließlich seiner Adresse, Telefonnummer, Zahlungsinformationen sowie jegliche weiteren Informationen, die durch Inanspruchnahme des Dienste beim Provider anfallen.

<sup>19</sup>Neben den Unterzeichnerstaaten ist auch Interpol dazu berechtigt, Anfragen an die Behörden eines Staates zu machen bzw. zu beantworten. (Artikel 27 Punkt 9 b) Europarat (vgl. 2001, S. 17)

## 4 Die Umsetzungen in Deutschland

Dass die Bundesrepublik Deutschland exemplarisch für das Vorzeigen der Probleme und Risiken der Umsetzungen in nationales Recht Verwendung findet, begründet sich wie bereits erwähnt darauf, dass sich für diesen Staat am meisten Literatur finden ließ. Darüber hinaus sind aber auch andere Mitgliedstaaten der EU nicht davor gefeit, den gleichen oder ähnlichen Problemen zu begegnen, sofern sie vergleichbare Gesetzestexte zu erlassen gedenken und identische Instrumente verwenden möchten.

Daneben gehen vor allem deutsche Sicherheitspolitiker davon aus, dass die BRD, neben Großbritannien wegen der vergleichsweise großen Zahl an Einsatztruppen in Afghanistan besonders gefährdet sei. Jörg Ziercke, der Chef des Bundeskriminalamtes (BKA) gibt die Zahl der terroristischen „Gefährder“ in Deutschland als zweistellig, „mit steigender Tendenz“ an. (vgl. Krempl & Briegleb, 2008a) Ob diese, aber auch Aussagen wie der Hinweis auf die bedeutende Gefahr eines terroristischen Anschlags mit nuklearem Material, einer sogenannten „schmutzigen Bombe“ der Realität entsprechen, oder, wie manche Wissenschaftler sagen, viel eher Panikmache als eine ernsthafte Bedrohung sind, das kann und sollte, zumindest zu Ungunsten der Bundesrepublik, nicht eindeutig festgestellt werden. (vgl. Krempl & Vahldiek, 2007)

Zu der sicherheitspolitischen Situation in der BRD lässt sich zudem grundlegend sagen, dass die großen Volksparteien sich von mehr Überwachung und schärferen Maßnahmen generell mehr Sicherheit erhoffen, wohingegen die Oppositionsparteien die Freiheits- und Bürgerrechte in den Vordergrund stellen. Entsprechend dem in Kapitel 1 beschriebenen Dilemma, fordert z.B. die CDU eine Aufhebung der Trennung von Polizei und Nachrichtendiensten. Interessanterweise kritisieren die Grünen, obschon sie die Anti-Terror-Gesetze in der vorigen Legislaturperiode als Regierungspartei mitgetragen haben, die von der derzeitigen großen Koalition verabschiedeten oder noch diskutierten Gesetzesvorlagen. „Integration, Dialog, Solidarität und Toleranz“ sind für die Grünen die besseren Sicherheitsmaßnahmen. (vgl. Umlauf, 2006)

### 4.1 Der biometrische Reisepass

#### 4.1.1 Details zur Umsetzung

Der biometrische Reisepass, auch als elektronischen Pass (ePass) bezeichnet, ist in der Bundesrepublik Deutschland, gemäß den Vorgaben der EU-Verordnung, mit einem passiv funkenden RFID-Chip ausgestattet. Wenngleich schon seit 2006 biometrische Daten wie Gesichtsbild und seit 2007 auch die Fingerabdrücke aufgenommen und in das Reisedokument integriert werden, ist der Vergleich der biometrischen Merkmale in den Pässen mit den entsprechenden Daten des Inhabers erst ab 2009 vorgesehen. Denn erst dann ermöglicht die Ausrüstung der Grenzkontrollstellen mit den passenden Lesegeräten, eine angeblich bessere Identitätsprüfung. (vgl. Krempl & Briegleb, 2007a)

Die Entscheidung, Fingerabdrücke neben dem Gesichtsbild als biometrisches Merkmal auf dem Reisepass zu speichern, fiel Ende Mai 2007 im deutschen Bundestag. Seit dem 1. November 2007 muss jeder Antragssteller auf einen Reisepass auf den Passbehörden die Fingerabdrücke seiner zwei Zeigefinger anfertigen lassen. (vgl. Krempl & Briegleb, 2007c, S. 41) Auch ist die Eintragung eines Kindes auf den elterlichen Pass seitdem nicht mehr möglich. Für Kinder unter 12 Jahren sind gesonderte Reisedokumente mit einer Gültigkeitsdauer von sechs Jahren vorgesehen, Kinder ab 12 Jahren sollen dahingegen auch biometrische Pässe bekommen. Elektronische Pässe einschließlich Fingerabdrücken sind allerdings erst ab 6 Jahren erhältlich. (Krempl & Kuri, 2007c) Diese doch beachtenswert tiefe Altersgrenze macht offensichtlich, dass die biometrischen Pässe nicht ausschließlich dem Zweck der Bekämpfung des internationalen Terrorismus dienen sollen.

Der Sinn eines derart teuren Reisedokumentes wurde auch wiederholt in Frage gestellt. Vor allem, da die deutschen Reisepässe bereits vor der Einführung des ePasses als die mitunter sichersten Reisepässe galten. So hatte die Bundesregierung im Sommer 2007 noch im deutschen Bundestag erklärt, dass bisher keine deutschen Ausweisdokumente von Terroristen benutzt worden seien und es seit dem Jahr 2000 auch nicht zu einer nen-

nenswerten Zahl von Fälschungen deutscher Pässe gekommen sei<sup>20</sup>. (vgl. Krempl & Kuri, 2007c) Auch dies erlaubt berechtigte Zweifel an der Argumentation, die Aufnahme biometrischer Daten in die Reisepässe sei eine effektive Maßnahme im Kampf gegen der Terror.

Von deutschen Politikern, wie z.B. dem Innenexperten Clemens Binniger (CDU), wird allerdings auch kein Geheimnis daraus gemacht, dass der biometrische Pass neben der vermeintlichen Erhöhung der Sicherheit auch ein Standortfaktor für Deutschland ist. (vgl. Krempl & Briegleb, 2007c, S. 41) Offensichtlich sei, so ein Sprecher des in Berlin ansässigen CHAOS COMPUTER CLUB (CCC), „dass die Sanierung der durch fehlgeschlagene Privatisierung ruinierten Bundesdruckerei und die Förderung der deutschen Biometrieindustrie hier eine viel wichtigere Rolle spielen, als das Streben nach Sicherheit.“ (Rosengart, 2005) In der Tat hat das im Besitz der LANDESBANK HESSEN-THÜRINGEN befindliche Unternehmen im Geschäftsjahr 2006 einen Umsatzsprung von 215 auf 262 Millionen Euro verzeichnen können. Der Gewinn der Bundesdruckerei stieg dementsprechend von 27,2 Millionen auf 63,7 Millionen Euro. (Borchers & Ziegler, 2007)

Der CCC bezeichnet den elektronischen Pass schlicht und einfach als Experiment zur „biometrischen Vollerfassung der Bevölkerung“ (vgl. Krempl, 2008, S. 20)

#### 4.1.2 Politische Versprechen und die Rasterfahndung

Wie bereits im Kapitel 3.1 auf Seite 8 besprochen, erlaubt Artikel 4 Absatz 3 der Verordnung über biometrische Reisedokumente die Verwendung der Daten ausschließlich zur Feststellung der Identität des Inhabers. In diesem Sinne wurde den Bürgern der Bundesrepublik vom ehemaligen Innenminister Otto Schily (SPD) auch zugesichert, dass die digitalen Lichtbilder ausschließlich im Chip des Dokumentes gespeichert werden würden. Die Merkmale würden nur der Identifizierung des Inhabers dienen und könnten nicht einmal zu Fahndungszwecken benutzt werden. (vgl. Wilkens, 2007) Dennoch beinhaltete die fertige Regelung die Vorgabe, dass das Bild beim Passregister zu speichern sei. (vgl. Krempl & Kuri, 2007d)

Auf die Frage eines TAZ-Reporters, wie lange das Versprechen, die biometrischen Daten aus den Datenbanken nicht zu Fahndungszwecken verwenden zu wollen, denn nun gelte, lautete die lakonische Antwort des derzeitigen Bundesinnenministers Wolfgang Schäuble (CDU):

*„Der Gesetzgeber behält immer die Möglichkeit, einmal getroffene Entscheidungen später zu revidieren. Da lege ich mich jetzt nicht fest.“* (Wolfgang Schäuble, zit. n. Rath, 2007)

Entgegen der Versprechen sollen die Gesichtsfotos denn nun nicht nur bei Ordnungswidrigkeiten im Straßenverkehr, sondern auch zur Verfolgung von Straftaten der Polizei zur Verfügung stehen. (REBUILD) Eine automatisierte Online-Übermittlung soll zwar nur im Eilfall und bei Nicht-Erreichbarkeit der 5300 Meldestellen möglich sein, doch diese Erfordernisse werden wohl 16 Stunden am Tag gegeben, und damit dem automatisierten Abruf Tür und Tor geöffnet sein. (vgl. Krempl & Briegleb, 2007c, S. 41) In der Praxis führt diese Ermächtigung dann auch zu einer Zentraldatei, die man durch das Speichern der Bilder bei den jeweiligen Passbehörden eigentlich verhindern wollte. Die Polizei kann Daten abrufen, ohne dass jemand kontrolliert, ob die Abfrage berechtigt war oder nicht. (vgl. Krempl & Kuri, 2007d)

Doch es soll nicht beim Zugriff auf die Fotos bleiben. Denn Schäuble schlägt vor, auch die Fingerabdrücke, die bisher nur im RFID-Chip des ePasses gespeichert sind, auch bei den Meldeämtern zu hinterlegen. Auch der CDU-Innenexperte Clemens Binniger spricht sich für eine solche Maßnahme aus. (vgl. Krempl & Briegleb, 2007c, S. 41) Datenschützer und die SPD laufen dagegen allerdings Sturm. (vgl. Krempl, 2007c, S.40) Eine solche Maßnahme würde die Meldedaten mit den Kriminalregistern des BKA gleichsetzen. Sogar die deutschen Polizeigewerkschaften halten solche „erkennungsdienstliche Behandlungen der Gesamtbevölkerung“ für übertrieben und ungerechtfertigt. Das Recht des Einzelnen auf „informationelle Selbstbestimmung“ wäre damit nicht

<sup>20</sup>Konkret wurden nach Auskunft der Bundesregierung zwischen 2001 und 2006 nur 6 Fälschungen und 344 Verfälschungen deutscher Pässe festgestellt. Und dies, obwohl in diesen Jahren bereits „erhöhte Terrorgefahr“ bestand. Borchers & Kuri (2007b)

mehr gewährleistet und die Verhältnismäßigkeit von Bürgerrechten und Sicherheitsinteressen des Staates nicht mehr gewahrt. (vgl. Krempl, 2007c, S.40)

#### 4.1.3 Sicherheitsrisiko statt Sicherheitmaßnahme?

Die grundlegende Idee hinter dem ePass ist laut EU-Verordnung also die eindeutige Identität einer Person festzustellen. Bei terroristischen Angriffen war das Problem jedoch bisher nicht, dass Personen unter falscher Identität innerhalb der Staaten mit biometrischen Pässen gereist wären<sup>21</sup>. Ein biometrischer Pass wird auch entgegen aller noch so hohen Erwartungen niemals die (potentiell böswilligen) Absichten einer Person offenbaren. Walter Peissl vom Wiener Institut für Technikfolgenabschätzung (ITA) Peissl (vgl. 2002, S. 7) streicht in seinem Beitrag für alle Überwachungsmaßnahmen<sup>22</sup> zu Recht hervor, dass Überwachung ex-ante kein abweichendes, also auffälliges Verhalten aufdecken kann.

Auf der anderen Seite gehen von der Sammlung biometrischer Merkmale eine ganze Reihe bedeutender Gefahren aus. So könnten z.B. durch die Abfrage der Merkmale bei Kontrollstellen und Ausreisen und deren anschließender Speicherung Bewegungsprofile der Passinhaber erstellt werden, welche nicht mit Freiheitsrechten in einer liberalen Gesellschaft in Einklang zu bringen sind. Auch geht von den elektronischen Pässen zunächst die Gefahr aus, dass von ihnen unbemerkt Daten abgefragt werden könnten, da die Abfrage über Funk abgewickelt wird. (vgl. Gamper, 2007, S. 23)

Das unbemerkte Auslesen soll zwar durch die verwendeten Sicherheitsvorkehrungen unmöglich gemacht werden, doch das wurde bereits bei der ersten Generation der biometrischen Pässe, die mit einem Basic Access Control (BAC) genannten System geschützt wurden, behauptet. Bei diesem System können die Daten vom Reisepass nur entschlüsselt werden, wenn Geburtsdatum, Ablaufdatum und Passnummer bekannt sind, man also physikalischen Zugang zum Dokument hat. Doch unabhängigen Forscherteams in Belgien und den Niederlanden ist es bereits nach kurzer Zeit gelungen, die Pässe auszulesen oder gar zu klonen. Die erste Generation der belgischen Reisepässe, die zwischen Ende 2004 und Mitte 2006 herausgegeben wurde, verfügten erschreckender Weise über keinerlei Schutzfunktion. Das Foto wie auch die digitalisierte Unterschrift des Inhabers konnten von Forschern der Katholischen Universität Louvain innerhalb von Sekunden unbemerkt ausgelesen werden. (Bachfeld, 2007) Das niederländische Team hingegen, hat es sogar geschafft, mit einem handelsüblichen Computer die BAC Verschlüsselung der Reisepässe innerhalb von nur 3 Stunden zu knacken. Möglich war dies, weil die Zahl der monatlich ausgegebenen Pässe nahezu konstant ist und dadurch ein linearer Zusammenhang zwischen dem Ausgabedatum und der Passnummer festgestellt werden konnte, der die Effektivität des Schlüssels bedeutend senkt. (vgl. Rütten, 2006)

Da die erste Generation des deutschen Reisepasses das gleiche Verschlüsselungsverfahren anwendet, sind auch diese nicht sicher. Der Sicherheitsexperte Lukas Grunwald hat auf der Sicherheitskonferenz BLACK HAT BRIEFINGS AND TRAINING USA 2006 am 3. August 2006 in Las Vegas vorgeführt, wie man biometrische Pässe mit Hilfe der offiziellen Referenzimplementierung der Software<sup>23</sup> und einem offiziellen Lesegerät klonen kann. Das Klonen an sich ist wenig spektakulär und sogar in der ICAO Dokumentation vorgesehen, aber es stellt ein Risiko dar und bietet potentiellen Angreifern einen großen Spielraum an Angriffspunkten. (vgl. Lettice, 2006; Ziegler, 2006) Nicht einmal der vorhin erwähnte physikalische Zugriff auf die Dokumente oder das Wissen über einen linearen Zusammenhang zwischen Ausstellungsdatum und Passnummer ist zwingend nötig. So stehen die zum Auslesen des Passes benötigten Daten auch anderen Organisationen zur Verfügung. Hotels, Banken,

<sup>21</sup>Siehe dazu auch die Auskunft der Bundesregierung in Kapitel 4.2.1

<sup>22</sup>„This is true for telecommunications wiretapping and eavesdropping as well as for video-surveillance of public places and for the biometric methods that are in discussion all over the world. Electronic fingerprints or iris-scans can only tell you something about the authenticity of a person. However, if the person did not attract attention yet, she will never be in a database and therefore cannot be detected as 'suspicious'." Peissl (2002, S. 8)

<sup>23</sup>Mehr Informationen zu dieser GOLDEN READER TOOL genannten Software findet sich auf der Homepage des BUNDESAMTES FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: <http://www.bsi.bund.de/literat/faltbl/F25GRT.htm>

Mobilfunkanbieter u.s.w. speichern diese Daten, zum Teil unkontrolliert und ungesichert. (vgl. Behme, 2006)

Die EU hat unter anderem deshalb für Reisepässe mit Fingerabdrücken die Extended Access Control (EAC) vorgeschrieben. Die erweiterte Sicherungstechnik sieht nämlich vor, dass sich die Lesegeräte mittels eines Zertifikats als Authentisch ausweisen müssen. Und diese Zertifikate wird ausschließlich das Bundesamt für Sicherheit in der Informationstechnik vergeben. (vgl. Krempl & Kuri, 2007c) Nur mehr das Zusammenspiel dieses Zertifikats mit einem besonderen Schlüssel auf dem Pass können den RFID-Chip noch dazu bewegen seine Daten preis zu geben und ihre Echtheit zu garantieren. (vgl. Krempl & Briegleb, 2007b) Nach Angaben des CDU-Innenexperten Clemens Binniger soll die Sicherheit des Chips für die nächsten 20 Jahre gewährleistet sein, die Zeit wird zeigen ob das kleine Funk- und Speichermedium diesen Ansprüchen gerecht werden und den Knackversuchen standhalten wird können. (vgl. Krempl & Briegleb, 2007c, S. 41)

Neben dem Auslesen und Klonen der Reisepässe, gibt es aber noch eine ganz andere Gefahr: Datenschützer warnen vor Betrügereien mit biometrischen Merkmalen im großen Stil. Der CHAOS COMPUTER CLUB (CCC) hat bereits wiederholt gezeigt<sup>24</sup>, wie einfach Fingerabdrücke „gestohlen“ und kopiert werden können. Medienwirksam wurden so bereits erfolgreich die Fingerabdruck-Scanner der Edeka Märkte getäuscht. (vgl. Krempl, 2008, S. 22) Und wer Fingerabdrücke wirklich und absolut benötigt, der wird auch nicht davor zurückschrecken sich die entsprechenden Gliedmaßen bei Bedarf zu besorgen. (vgl. Schulz, 2008) Statt den Identitätsmissbrauch zu verhindern, warnen Datenschützer, könnte das Großprojekt Biometrie viel eher einem professionel geplanten Identitätsdiebstahl Vorschub leisten. Kriminelle oder auch Geheimdienste könnten Fingerabdrücke sammeln und sie als falsche Hinweise an Tatorten verteilen, um so Verwirrung zu stiften und die Ermittler in die Irre zu führen. (vgl. Krempl & Briegleb, 2007a; Krempl & Ziegler, 2007b) BKA-Präsident Jörg Ziercke hält dagegen und meint:

*„[f]ür die mutwillige Verschleierung von Straftaten durch falsche Fingerabdrücke etwa gebe es überhaupt keine Beweise.“*(Jörg Ziercke zit. n. Krempl & Ziegler, 2007b)

#### 4.1.4 Was taugt der biometrische Pass?

Die hochgelobte Technologie hat sich unterdessen auch als alles andere als unfehlbar erwiesen. Bei Tests mit den biometrischen Pässen musste festgestellt werden, dass je nach Verfahren zwischen 3 und 23 Prozent der teilnehmenden Personen nicht mit den Merkmalen in ihren Reisedokumenten identifiziert werden konnte. (vgl. Rosengart, 2005) Auch eine Studie der LONDON SCHOOL OF ECONOMICS, an der 10.000 Freiwillige teilnahmen, bestätigte, dass das System bei rund 20 Prozent der Fingerabdrücke versagt. (vgl. Batarilo, 2006) Überhaupt seien die biometrischen Merkmale auf den RFID-Chips vermutlich nur für fünf Jahre verwendbar; die Gültigkeit des Passes beträgt in Deutschland jedoch zehn Jahre<sup>25</sup>. (vgl. Krempl & Ziegler, 2007b) Auf eine alltägliche Situation hochgerechnet, würde dies bei zehntausenden Menschen an den Flughäfen zu Falschmeldungen führen. Wer nicht als legitim erkannt wird, gerät unter Rechtfertigungsdruck. Zudem wäre ein Teil der Bevölkerung, der von Natur aus schlecht erfassbare Fingerabdrücke hat, einer regelmässigen und unumgänglichen Diskriminierung ausgesetzt. (vgl. Rosengart, 2005; Batarilo, 2006)

Ob die biometrischen Pässe ihren Zweck erfüllen werden, daran Zweifeln die Experten des CCC allesamt. Frank Rosengart (vgl. Rosengart, 2005) und Constanze Kurz (zit. n. Krempl & Ziegler, 2007a) sind davon überzeugt, dass der Einsatz von Funkchips und Biometrie das Sicherheitsniveau des, „dank modernster Druck- und Holografie-Technologien“, ehemals zu den sichersten Reisepässen der Welt gehörenden deutschen Reisepasses senken wird. Auch aus dem Grund, dass sich die Grenzbeamten zunehmend auf die unausgereifte Technik

<sup>24</sup>Eine Anleitung als Video und Fotoabfolge ist unter [http://www.ccc.de/biometrie/fingerabdruck\\_kopieren.xml?language=de](http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=de) zu finden.

<sup>25</sup>Der luxemburgische ePass des Autors, sowie die Pässe seiner luxemburgischen Bekannten haben allerdings nur eine fünf-jährige Gültigkeit.

verlassen werden.

## 4.2 Die Vorratsdatenspeicherung

### 4.2.1 Details zur Umsetzung

Die Zahl der Abfragen von Verbindungsdaten stieg in den letzten Jahren in Deutschland auch ohne Vorratsdatenspeicherung rasant. Von 2006 auf 2007 konnte sogar ein Anstieg um 60% verzeichnet werden. Dennoch wurde am 9. November 2007 im deutschen Bundestag die Umsetzung der Vorratsdatenspeicherungsrichtlinie in Form einer Telekommunikationsgesetznovelle gestimmt. Seit dem 1. Jänner 2008 sind Telekommunikationsbetreiber dazu verpflichtet, Rufnummer, Uhrzeit und Datum der Verbindung vorrätig zu halten. (vgl. Krempl, 2007a, S. 60) Internetprovider müssen bei jedem Zugang zum Internet, egal ob World-Wide-Web, Voice-over-IP (VoIP) oder Email, Beginn und Ende der Nutzung sowie die dabei zugeordnete IP-Adresse für 6 Monate speichern. Auch jeder bloße Zugriff auf das Email-Postfach muss mit Zeitpunkt und IP festgehalten werden, bei Empfang einer Email, fällt die IP-Adresse des Absenders ebenfalls unter die zu speichernden Daten. Rechtlich fragwürdig ist die Speicherung der Kopfzeile, denn diese enthält neben dem eingeschlagenen Pfad und weiteren Informationen auch die Betreffszeile - eigentlich sind das Inhaltsdaten. (vgl. Krempl, 2007f,a, S. 52; S. 60)

Die Vorratsdaten sollen in Deutschland entgegen den EU-Vorgaben auch zur Aufklärung minder schwerer Straftaten genutzt werden dürfen. (vgl. Krempl, 2007b, S. 50) Die deutsche Bundesjustizministerin Brigitte Zypries sieht die Vorratsdatenspeicherung auf jedenfall nicht als weiteren Pflasterstein auf dem Weg zum Überwachungsstaat, denn es würden ja bloß die Daten gespeichert werden, die ohnehin bei den jeweiligen Dienstleistern anfallen<sup>26</sup>. Weiters wurde behauptet, die EU-Richtlinie sei in „minimaler Weise“ umgesetzt worden, obwohl die Richtlinie um einige Straftaten aus dem Telekommunikationsbereich ergänzt wurde. (vgl. Krempl, 2007a, S. 60) Zugriff auf diese Daten haben in der BRD Staatsanwaltschaft, Polizei und Geheimdienste, und das ohne richterlichen Beschluss. (vgl. Krempl, 2007b, S. 50) Wie bereits angedeutet, sollen diese Behörden nicht mehr nur zur Strafverfolgung, sondern ebenfalls „zur Abwehr von erheblichen Gefahren“ und „zur Erfüllung der gesetzlichen Aufgaben der Geheimdienste“ auf die Vorratsdaten zurückgreifen dürfen. Auch strafrechtlich relevante Urheberrechtsverletzungen sind dabei eingeschlossen, nicht jedoch deren zivilrechtliche Pendant. Politiker der CDU und die Musikindustrie stehen jedoch schon in den Startlöchern, um die Verwendung der Daten auch zu diesem Zweck durchzusetzen. (vgl. Krempl, 2007f,b)

Ähnlich wie bei der Diskussion um den biometrischen Pass, wird auch bei der Vorratsdatenspeicherung darüber debattiert, ob die Daten nun dezentral bei den Providern oder in einer zentralen Datenbank zu speichern seien. Die Bspitzelungsaffäre bei der Deutschen Telekom hat viele davon überzeugt, dass die Daten in einem zentralen „Sicherheits-Center“, unter Aufsicht des Datenschutzbeauftragten, besser aufgehoben wären, also bei den Dienstleistern. Der Vorsitzende des Bundes Deutscher Kriminalbeamter (BDK), Klaus Jansen, bemängelt, dass die Daten bei privaten Unternehmen offensichtlich „mehr als schlecht aufgehoben“ seien. Auf die Zentral-Datenbank könnten dann sowohl der Staat zur Strafverfolgung als auch die Unternehmen zu Abrechnungszwecken zugreifen. (vgl. Kuri, 2008)

### 4.2.2 Was bringt die Vorratsdatenspeicherung?

Unterdessen hagelt es aber auch berechtigte Kritik an der Vorratsdatenspeicherung, und dies nicht nur aus Richtung der Datenschützer. Laut einer Studie des BKA könnte sich die Aufklärungsquote von Kriminalfällen, die derzeit bei 55% liegt, durch die Vorratsdatenspeicherung auf bestenfalls 55,006% erhöhen. Zu einem ähnlichen Ergebnis kommt auch eine Studie des Max-Planck-Instituts für Strafrecht. Hätten für die Ermittlungsarbeit an Strafverfahren in den Jahren 2003 und 2004 bereits Vorratsdaten zur Verfügung gestanden, dann wären lediglich

<sup>26</sup>Dem Autor fällt es allerdings schwer, den Sinn dieser Aussage zu begreifen. Mehr als die „sowieso“ bei Zugangsanbietern generierten Daten gibt es praktisch nicht und ob sie „ohnehin“ anfallen oder nicht, steht weder in einem logischen Zusammenhang zu ihrer Relevanz noch begründet es einen Kausalzusammenhang zwischen Generierung und Speicherung.

0,01% der 4,9 Millionen Ermittlungsverfahren mehr gelöst worden. (vgl. Krempf & Wilkens, 2008a) Der Jurist Patrick Breyer erklärte, dass die Aufklärungsquote von Verbrechen im Internet bereits vor der Einführung der Vorratsdatenspeicherung bei 80% lag, wesentlich höher also als bei den traditionellen Verbrechen. (vgl. Krempf, 2007g, S. 85) An dieser Stelle sei deshalb einmal mehr auf die angebliche Verhältnismäßigkeit der Vorratsdatenspeicherung hingewiesen und in Frage gestellt, ob sie mit Verweisen auf den rechtsleeren Raum Internet zu rechtfertigen ist.

Es mag an diesen schlechten Werten liegen, dass die Vorratsdatenspeicherung sogar dort gelobt und als berechtigt erklärt wird, wo sie überhaupt nicht zum Einsatz gekommen ist. Ein CDU-Politiker behauptete, die Festnahme der zwei Täter, die im Dezember in einer Müncher U-Bahn einen Rentner überfielen sei mittels Vorratsdaten erfolgt, dabei war zu dem Zeitpunkt, als die beiden Jugendlichen festgenommen wurden, das Gesetz noch überhaupt nicht in Kraft. Sie wurden anhand eines gestohlenen Mobiltelefons aufgestöbert. (vgl. Muehlbauer, 2008)

Dabei ist die Vorratsdatenspeicherung leicht zu umgehen. Ein Webmail Angebot ausserhalb der EU reicht schon, um der Speicherung der Email-Daten zu entgehen. (vgl. Krempf, 2007f, S. 52) Auch anderen Möglichkeiten, der Erfassung zu entgehen, gibt es wie Sand am Meer. Das Verwenden eines oder sogar mehreren Vermittlungsservern, sogenannten *Proxies*, verhindert die eindeutige Zuordnung von aufgerufenen Diensten zu einem Internetnutzer. Nur die Verbindungen zum Proxy und die vom Proxy zum Dienst können protokolliert werden, was sich im Proxy abspielt, welcher Benutzer genau welche Seite aufgerufen hat ist nicht mehr nachvollziehbar sobald mehr als eine Person den Proxyserver verwendet<sup>27</sup>. Unscharf wird Korrelierung unterschiedlicher Datensätze aber auch dadurch, dass auf vielen Geräten unterschiedliche Zeitzonen eingestellt sind und sich somit rasch Fehler bei der Auswertung von IP-Adressen zu Stammdaten ergeben können. (vgl. Larnhof, 2006, S. 24)

Die Verhältnismäßigkeit der Vorratsspeicherung ist auch durch die dadurch entstehenden Kosten in Frage gestellt. Geht man davon aus, dass pro Benutzer und Monat 50 Megabyte an Vorratsdaten zusammenkommen (vgl. Larnhof, 2006, S. 50), dann wären das in Deutschland in einem Monat, bei 42,7 Millionen Internetnutzern (vgl. Fischer, 2008) ganze 1,988 Petabyte<sup>28</sup> an Vorratsdaten. Da die Daten 6 Monate lang aufbewahrt werden müssen, versechsfacht sich diese wahnsinnige Menge auf noch gigantischere 11,93 Petabyte<sup>29</sup>. Bei einem derzeit gültigen Preis von ungefähr € 0,15 per Gigabyte (vgl. alt, 2008) würden sich die Kosten für Speicherplatz alleine auf € 1.876.465 belaufen. Dabei sind die Kosten für die Festplatten aufnehmenden Servercomputer oder die Gehälter für mindestens eine zusätzliche Arbeitskraft noch gar nicht mit eingerechnet.

### 4.2.3 Verhältnismäßig und gerechtfertigt?

Ist es nunmehr also verhältnismäßig und gerechtfertigt, 100 Prozent der Bevölkerung bei der Nutzung elektronischer Kommunikationsmedien zu überwachen? Der Datenschützer Thilo Weichert ist davon ganz und gar nicht überzeugt, er hält diesen Generalverdacht für verfassungswidrig. (vgl. Krempf, 2007f, S. 53) Dementsprechend hat das Bundesverfassungsgericht (BVG) im März 2008 die Umsetzung der Vorratsdatenspeicherung etwas revidiert. Die deutschen Sicherheitsbehörden dürfen seitdem nur mehr bei begründetem Verdacht zur Verfolgung schwerer Straftaten auf die Vorratsdaten zugreifen. Und auch dies nur wenn die Ermittlung des Sachverhalts auf keine andere Art und Weise mit Aussicht auch Erfolg durchzuführen ist. (vgl. Krempf & Wilkens, 2008b) Die Vorratsdatenspeicherung stellt aber nicht nur die gesamte Bevölkerung unter Tatverdacht, sie kann noch dazu zu einer Falle für Unschuldige werden. Unter anderem durch das Abfangen von Passwörtern (Phishing)

<sup>27</sup>Es sei denn, der Proxy wäre absichtlich in das Netz eingeschleust worden. Dann könnten die Daten, sofern sie nicht verschlüsselt sind, natürlich mitgehört werden. Auch durch ein sehr aufwendiges, langwieriges und ressourcenhungriges Verfahren, der Analyse der Verkehrsdaten (Traffic Analysis) könnten möglicherweise die Anfragen des Benutzers wieder diejenigen des Proxys zugeordnet werden. Grundsätzlich lässt sich beim Mit-"hören" von unverschlüsselten Inhaltsdaten die Identität eines Nutzers immer feststellen, aber dabei bewegen wir uns aus dem Bereich der Vorratsdatenspeicherung.

<sup>28</sup>Respektiv 2036 Terabyte oder 2.084.961 Gigabyte

<sup>29</sup>Equivalent zu 12.216,6 Terabyte oder 12.509.765,6 Gigabyte. Das sind rund 2.843.128 prall gefüllte DVDs

könnten Ahnungslose unter Verdacht geraten. Der, noch dazu im Umgang mit dem Internet wahrscheinlich unerfahrene oder naive Benutzer muss dann beweisen, dass seine Daten ausgespäht wurden. Und das stellt sich zumeist als schwierig, wenn nicht sogar unmöglich heraus. (vgl. Larnhof, 2006, S. 61) Wir werden auf diesen Punkt aber noch einmal im Rahmen des Kapitels über die schwindende Unschuldsvermutung (6.1) näher eingehen.

### 4.3 Der „Bundestrojaner“

#### 4.3.1 Wozu Online-Durchsuchung?

Die Online-Durchsuchung ist verständlicherweise eines der am heißesten diskutierten Themen der Deutschen Sicherheitspolitik. Gründe für den Bundestrojaner, wie die Software mehr oder weniger ernsthaft unter Kritikern genannt wird, gibt es zu Hauf. So betitelt Jörg Ziercke das Internet als das entscheidende Kommunikationsmittel des internationalen Terrorismus. Die „Szene“ arbeite hoch konspirativ und verdeckt, sie verschlüssele und anonymisiere ihre Kommunikationsmittel, so dass man die Daten unbedingt schon vor der Verschlüsselung abfangen müsse. (vgl. Kuri, 2007a) Der Vorsitzende der Gewerkschaft der Polizei (GdP) weist ebenso darauf hin, dass „herkömmliche Ermittlungsmethoden, wie zum Beispiel Wohnungsdurchsuchungen“ (zit. n. Borchers & Kuri, 2007a), auch im nunmehr virtuellen Arbeits- und Wohnraum möglich sein müssten. Alleine in dieser scheinbar logischen Argumentationskette liegt jedoch schon ein Denkfehler, auf den wir im nächsten Punkt noch genauer eingehen werden. Innenminister Wolfgang Schäuble ist des weiteren der Ansicht, Strafverfolger sollten nicht künstlich dumm gehalten werden, sondern bei ihrer Ermittlungsarbeit alle technisch verfügbaren Mittel einsetzen dürfen. Die großen Gefahren, die der Terrorismus darstellt, verlangten nach mehr präventiver Strafverhinderung an Stelle von repressiver Strafverfolgung. (vgl. Krempl, 2007c, S. 38) Der hessische Innenstaatssekretär Harald Lemke ist der Ansicht, um Staatlichkeit ins Internet zu bringen sei die Online-Durchsuchung noch wichtiger als die Vorratsdatenspeicherung und alle anderen Maßnahmen. (Borchers & Kuri, 2008) Eingesetzt werden soll die Software, nach letzten Aussagen des BKA-Präsidenten Jörg Ziercke, 10, bis maximal 15 Mal im Jahr<sup>30</sup>. (vgl. Krempl & Kuri, 2008a)

#### 4.3.2 Fehlende rechtliche Grundlagen

Zweifel der Opposition oder gar der Koalitionspartner an der Notwendigkeit einer solchen Maßnahme wurden mit öffentlichkeitswirksamen Festnahmen von Terrorverdächtigen aus dem Weg geräumt. Ob diese Festnahmen, die darüber hinaus ohne Online-Durchsuchung durchgeführt werden konnten, aus purem Zufall in Deutschland wie auch in Österreich jeweils kurz vor Debatten in den jeweiligen Parlamenten durchgeführt wurden, darüber kann man nur schelmenhaft spekulieren. Auf jeden Fall untermauerten die von den geplanten Bombenanschlägen ausgehenden Gefahren den „Anschein“, dass der Verzicht auf die Online-Durchsuchung ein hohes Sicherheitsrisiko darstellt. Kuri (vgl. 2007b)

Doch die Umsetzung der, in der Cybercrime Convention geforderten, Zugangsberechtigungen der Ermittlungsbehörden zu Computersystemen und Datenträgern gestaltete sich in Deutschland komplizierter als man sich erhofft hatte. Bereits im November 2006 wurde die heimliche Durchsuchung von Festplatten für unzulässig erklärt. Die verdeckte Online-Durchsuchung, so die Begründung, sei nicht mit einer offenen Hausdurchsuchung, sondern eher mit dem heimlichen Abhören von Wohnungen zu vergleichen. Daher ist schon der Begriff „Online-Durchsuchung“ fehlleitend, da es sich bei der Durchsuchung einer Wohnung um eine einmalige Aktion handelt, bei der der Beschuldigte oder ein Vertreter sowie Zeugen anwesend sein müssen. Die Online-Durchsuchung hin-

<sup>30</sup>Im Sommer 2007 sprach Ziercke noch von 20 Einsätzen pro Jahr

gegen soll unerkannt und über einen längeren Zeitraum stattfinden, es handelt sich also hierbei in der Tat eher um eine Abhöraktion. Magnus (vgl. 2007, S. 103)

Der Bundesgerichtshof bekräftigte dieses Urteil am 5. Februar 2007. Er untersagte die Durchsuchung privater Computer durch die Polizei wegen fehlender rechtlicher Grundlagen. (vgl. Kuri, 2007d; Borchers, 2006) Der SPD Innenexperte Dieter Wiefelspütz gibt demnach zu bedenken, dass die Online-Durchsuchung weder eine Hausdurchsuchung, noch eine Abhörmaßnahme, sondern vielmehr etwas Drittes ist, für das noch keine klare Rechtsgrundlage besteht. (Borchers & Kuri, 2007a) Das BVfG hat die Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz, wo sie unabhängig vom Bund bereits eingeführt worden war, für verfassungswidrig erklärt und in Zuge dessen ein neues Grundrecht auf "Gewährleistung der Vertraulichkeit und Integrität" informationstechnischer Systeme ins Leben gerufen. Krempf & Kuri (vgl. 2008c) Die Richter verlangen zudem, dass die verdeckte Durchsuchung von Computern nur bei „konkreten Hinweisen auf Gefahr für hochrangige Rechtsgüter“ für zulässig erklärt und das Verfahren streng kontrolliert wird. Das Ausspähen von Privat-Computern soll nur mit richterlicher Genehmigung erlaubt und die Daten im Nachhinein von Ermittlungsrichtern, Staatsanwälten oder Justizbeamten ausgewertet werden, um sicher zu stellen, dass keine persönlichen Daten enthalten sind. Um diese Zusatzarbeit zu leisten, würden in der BRD allerdings 4.000 Richter und Staatsanwälte fehlen, deren Posten die Politik erst einmal schaffen müsste. (vgl. Krempf & Kuri, 2008d)

Die Online-Durchsuchung ist unterdessen auch nicht mit der Telekommunikations- oder der Email-Überwachung gleich zu setzen. Paragraph 100a der Strafprozessordnung (StPO), 1968 unter dem Namen „Telekommunikationsüberwachung“ eingeführt, erlaubt in Fällen von „überragendem Unrecht“ den Eingriff in das Fernmeldegeheimnis. Mehr als 2 Dutzend Mal wurde in diesem Kontext der Deliktskatalog bereits erweitert, was die Beschränkung auf Fälle von „überragendem Unrecht“ beträchtlich aufgeweicht hat. Paragraph 94 StPO erlaubt je nach Interpretation die „Beschlagnahmung“ von Emails, sofern sie nicht unterwegs sind, sondern sich auf einem Server befinden. Auf die reale Welt umgemünzt würde dies bedeuten, dass die Polizei aus einem an einer roten Ampel haltenden Postauto Briefe nehmen dürfte. (vgl. Störing, 2008, S. 156)

Fortan erklärten Innenminister Schäuble und das BKA die Schaffung einer gesetzlichen Basis zum frühestmöglichen Termin, notfalls durch eine Verfassungsänderung, als ein augenblicklich anzustrebendes Ziel. (vgl. Kuri, 2007d; Borchers, 2006) Der Regierungsentwurf des Gesetzestextes der diese rechtliche Grundlage enthalten soll, die BKA-Novelle, sorgt im Bundestag nach wie vor für feurige Kontroversen. (vgl. Störing, 2008, S. 156) Mit der Verabschiedung der Novelle ist frühestens 2009 zu rechnen, denn einige strittige Punkte sollen nach Auffassung der SPD noch korrigiert werden. So soll etwa nach dem derzeitigen Entwurf für muslimische Geistliche kein Abhörschutz bestehen. Auch soll die Kontrolle von Online-Durchsuchungen von BKA-Beamten anstelle von unabhängigen Gutachtern durchgeführt werden. Die CDU/CSU Fraktion sträubt sich allerdings vehement gegen eine Abänderung ihres Entwurfs. (vgl. Borchers & Briegleb, 2008)

Die verdeckte Online-Durchsuchung wird in Paragraph 20k des Gesetzesentwurfs als „verdeckter Eingriff in informationstechnische Systeme“ bezeichnet. Der Paragraph erteilt dem BKA das Recht, „ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme ein[z]ugreifen und aus ihnen Daten [zu] erheben“. Die Maßnahme soll unterdessen auf Gefahren für "Leib, Leben oder Freiheit einer Person" beschränkt werden und von einem Richter angeordnet werden müssen. Handelt es sich aber um Gefahr im Verzug, soll auch der BKA-Präsident oder dessen Vertreter eine Anordnung treffen können, die dann zunächst 3 Tage gültig wäre. (vgl. Krempf & Ziegler, 2008b) Die REMOTE FORENSIC SOFTWARE (RFS), wie die Software offiziell heißen wird, soll *zunächst* nur vom BKA und ausschließlich für die Bekämpfung des Terrorismus eingesetzt werden, nicht jedoch für die Aufdeckung von Straftaten, versicherte das Bundesinnenministerium zunächst. (vgl. Krempf, 2007c,d, S. 86) Wenig später wurde der Einsatz auch auf schwere Verbrechen wie Mord oder Kinderpornografie ausgeweitet. (vgl. Krempf, 2007d, S. 89) Den Politikern von CSU und CDU gehen diese Berechtigungen aber nicht weit genug. Sie fordern, den Bundestrojaner auch etwa gegen Hooligans einsetzen zu dürfen. (vgl. Ziegler, 2008) Speziell in Bayern fordert die CSU den Einsatz auch bei Bildung krimineller Vereinigungen, Geldfälschung und bei Drogendelikten einsetzen zu dürfen, wemgleich nur nach richterlicher

Anordnung, Kreml & Briegleb (vgl. 2008b)

Oppositionspolitiker, Datenschützer und Computerexperten lehnen den Einsatz der Online-Durchsuchung und ganz allgemein das Stimmen der BKA-Novelle vehement ab. Unter anderem, weil der Gesetzesentwurf ihrer Auffassung nach "eklatant gegen den bewährten Grundsatz der Trennung zwischen Polizei- und Geheimdienstarbeit" (Max Stadler, zit. n. Kreml & Briegleb, 2008c) verstoße. Das einzige Positive am Reformentwurf der StPO sei, dass der Katalog der Straftaten, bei denen eine Überwachung angeordnet werden kann, auf Vergehen mit Strafmaß über 5 Jahren Höchststrafe eingegrenzt werde. (vgl. Andresen, 2007, S. 98)

#### 4.3.3 Schwierigkeiten bei der Umsetzung

Doch ungeklärt ist immer noch, wie das „Tool zur Online-Durchsuchung“, das insgesamt nicht mehr als 200.000 Euro kosten soll, überhaupt auf den Rechnern der Verdächtigen landen wird. (vgl. Kuri, 2007d) Fest steht, darauf haben sich Innenminister Schäuble und Justizministerin Zypries nach langer Debatte geeinigt, dass die Polizei auf Bundesebene<sup>31</sup> nicht in Wohnungen einbrechen darf, um den Bundestrojaner auf privaten Rechnern zu installieren. Der Entwurf zur BKA-Novelle von Wolfgang Schäuble sah in Artikel 20t eben dieses Recht „auch zur Terrorabwehr eine Wohnung ohne Einwilligung des Inhabers betreten und durchsuchen zu dürfen“ vor. (vgl. Kreml, 2007d, S. 87) Was bleibt, ist eine Unmenge an anderen Möglichkeiten, denen aber allesamt nicht die nötige Wirksamkeit zugesprochen wird. Der CDU-Politiker Clemens Binniger bedauert diesen Umstand und gibt sich sichtlich enttäuscht: "Die Onlinedurchsuchung ist jetzt nur noch ein stumpfes Schwert" (Rath, 2008)

Unter den verbleibenden Maßnahmen ist so z.B. der Versand einer präparierten Email an den verdächtigen Computer-Nutzer. Sei ein begründeter Ausnahmefall gegeben, könne man nach Auskunft der Bundesministeriums für Inneres (BMI) die Email auch unter dem Namen einer anderen Behörde versenden. Bei entsprechendem Interesse würde der mutmaßliche Verbrecher, so hofft man, den Anhang öffnen und seinen Rechner unbewußt mit dem RFS infizieren. Als weitere Möglichkeit wird in Betracht gezogen, dem Benutzer eine CD zuzuschicken, die er ahnungslos in seinen Rechner einlegt. (vgl. Kreml & Briegleb, 2008b)

Entsprechend vorbereitete Internetseiten könnten die Software eventuell auch einschleusen, riskant nur, wenn ein unbescholtener Websurfer die Seiten mehr oder weniger zufällig ansteuern würde. Als vierte Möglichkeit sieht man die Vorgehensweise an, die Durchsuchungssoftware in ohnehin durchgeführte Downloads einzufügen. Das Verfahren wäre zwar subtil, durchleuchten könnte man es dennoch immer noch durch die Erweiterung der üblichen Sicherheitsvorkehrungen bei Downloads. Viele Programme müssten dazu nur einen automatisierten Vergleich der Prüfsummen ihrer Downloads durchführen. So ließen sich manipulierte Daten leicht entdecken und durch die Originaldaten ersetzen. Mit hoher Wahrscheinlichkeit würden auch die an der Einschleusung beteiligten Internetprovider und Softwarehersteller alsbald das Vertrauen ihrer Kunden verlieren. (vgl. Kreml, 2007d; Borchers & Briegleb, 2007, S. 87) Aus dem gleichen Grund ist es auch höchst unwahrscheinlich, dass Anti-Viren Software den Bundestrojaner absichtlich nicht erkennt. (vgl. Magnus, 2007, 102f) Sollte dies dennoch, entgegen jeder Wahrscheinlich eintreten, würde dies für findige Hacker<sup>32</sup> gleichermaßen einen Ansatzpunkt für Gegenmaßnahmen darstellen.

Auch kann nicht zu hundert Prozent sichergestellt werden, dass z.B. per Email verschickte Software auf dem vorgesehenen Rechner landet. Auch bei direkter Kommunikation mit dem Zielrechner ist nicht gewährleistet, dass man effektiv mit dem Rechner kommuniziert, dessen IP-Adresse man eingegeben hat<sup>33</sup>. (vgl. Dignatz, 2007, S. 100) Die Ermittler würden sich so unter Umständen auf einem in den USA befindlichen Server einloggen und damit, über die Grenzen Deutschlands hinweg, unzulässigerweise im Ausland bewegen. Störung (vgl. 2008, S.

<sup>31</sup>In Bayern wiederum soll sie dies dürfen. Kreml & Briegleb (vgl. 2008b)

<sup>32</sup>Der Begriff des Hackers wird hier nicht pejorativ verwendet. Vielmehr soll mit „Hacker“ eine technisch interessierte und zugleich versierte Person bezeichnet werden, die ein hohes Interesse an der Sicherheit von Computer-Systemen und -Software zeigt.

<sup>33</sup>Es ist an dieser Stelle weder möglich noch sinnvoll und angebracht, sich in die Details zu diesen Problemen zu vertiefen. Dem interessierten Leser seien trotzdem die Stichworte „IP Redirects“, „Network Address Translation (NAT)“ oder „Cloud Computing“ mit auf den Weg gegeben.

158) Der Zugriff auf außerterritoriale Geräte und Datenspeicher ist nämlich auch laut Artikel 32 der Cybercrime-Convention ohne die spezifische Erlaubnis des beherbergenden Staates nicht erlaubt. (vgl. Europarat, 2001, S. 20) Aus eben diesen Schwierigkeiten hatte das BKA zunächst vorgeschlagen, die RFS, wie bereits zuvor erwähnt, über einen physikalischen Zugriff auf die Hardware der Verdächtigen zu installieren.

Abseits der Gedanken, die man sich über das „Wie“ macht, ist auch die Frage des „Was“ längst nicht vom Tisch. BKA-Präsident Ziercke möchte die Bedenken gegen „unverhältnismäßige Grundrechtseingriffe bei Online-Durchsuchungen“ (Krempf, 2007c, S. 38) zerstreuen. Das Bundeskriminalamt soll mit eigens dafür entwickelter Software, auf Einzelfälle bezogen, gezielt vorgehen. Diese „Unikate“ (vgl. Krempf, 2007d, S. 88) sollen, so Ziercke weiter, auch keine „Schadsoftware“ im eigentlichen Sinne darstellen, und so auch keine Hintertüren, wie bei Trojanern ansonsten üblich, offen lassen. (vgl. Krempf, 2007c, S. 38) Das Programm werde überdies mit allen Firewalls und Anti-Viren Programmen getestet, damit es bei der Installation eben keinen Alarm schlägt<sup>34</sup>. Später werde sich das Programm selbst löschen um die Gefahr des Entdecktwerdens zu minimieren. (vgl. Borchers & Kuri, 2007d) Solche Aussagen lassen an den angestrebten Kosten von maximal € 200.000 schon Bedenken aufkommen. Zudem scheinen die Versprechen etwas weit hergeholt, wenn man bedenkt, dass es keine noch so professionelle Software gibt, die keine Schwachstellen wie z.B. Programmierfehler hat. Schwachstellen, so Constanze Kurz, die dann unter anderem von Kriminellen ausgenutzt werden könnten. Krempf (vgl. 2007c, S. 40) In einem derartigen Fall würde das BKA sogar die Vorarbeit für kriminelle Machenschaften leisten. Ziercke schließt auch den Rückgriff auf kommerziell erwerbliche Produkte nicht aus. (vgl. Krempf & Kuri, 2008a)

Zur Debatte der technischen Schwierigkeiten sei abschließend darauf hingewiesen, dass sich Terroristen oder „Cyberkriminelle“ sicher nicht absolut naiv im Internet bewegen, „jede mit Trojaner-Installern verseuchte Website [...] besuchen oder willenlos jeden Mailanhang anzuklicken.“ (Kuri, 2007a) Die sogenannten „Sauerland-Attentäter“ hätte man mit dem Bundestrojaner auch nicht überführen können, sie begaben sich bekanntermaßen hauptsächlich über Call-Shops und offene WLAN-Netze ins Internet, nicht über den eigenen Rechner. Krempf & Kossel (2007)

Ungeklärt, weil von den Verantwortlichen vermutlich als ausgeschlossen betrachtet, ist schlußendlich auch die Frage, wer bei Schäden Unschuldiger haftet. Potential für solche Schäden hätte das Projekt „Online-Durchsuchung“ auf jeden Fall. (vgl. Andresen, 2007, S. 98)

#### 4.3.4 Schutz der Privatsphäre

*"Auf den Computern von jungen Menschen findet sich mehr Privatsphäre als in den Schlafzimmern unserer Eltern"* (Markus Beckedahl, zit. n. Bihl, 2007)

Die Elterngeneration aber hätte nicht schlecht gestaunt, wenn der Staat ins Schlafzimmer geschaut hätte. Da der Schutz der Privatsphäre bei den Gerichtsurteilen über die Online-Durchsuchung so eine große Rolle spielt, wird das deutsche Innenministerium nicht müde zu beteuern, dass man durch technische Mittel Eingriffe in die Intimsphäre verhindern könne. Allerdings konnte dieses Versprechen bis dato noch nicht glaubhaft und konkret mit Fakten unterlegt werden. (vgl. Krempf, 2007d, S. 88) Bis zuletzt war man sich in Expertenkreisen auch darüber im Unklaren, ob bei einer Online-Durchsuchung das Grundrecht auf Unverletzlichkeit des Wohnraums oder aber eher das Recht auf informationelle Selbstbestimmung verletzt werden würde. (vgl. Krempf, 2007d, S. 89) Dem Juristen Johannes Rux nach ist das Aufzeichnen von Tastaturanschlägen und Mausbewegungen durchaus mit der Aufzeichnung des Verhaltens in einer Wohnung vergleichbar. Daher sei die Online-Durchsuchung, wie die Wohnraumüberwachung, nur dann zulässig, wenn sich durch deren Einsatz eine besonders dringende Gefahr verhüten ließe. (vgl. Borchers & Kuri, 2007c)

<sup>34</sup>Gute Schutzprogramme analysieren aber das gesamte System und melden auffälliges Verhalten von Programmen.

Durch die Schaffung des neuen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat das Bundesverfassungsgericht dieses Dilemma gelöst. Problematisch bleibt aber weiterhin, dass der Staat sich durch den Bundestrojaner Zugriff auf das gesamte Leben seiner Einwohner verschaffen könnte. Der FDP-Politiker Ulrich Goll hält die Online-Durchsuchung für einen weiteren Schritt in Richtung Überwachungsstaat. Er findet es „naiv zu glauben, dass Terroristen ihre Bombenbaupläne auf eine Festplatte speichern, die ans Internet angeschlossen ist“. (zit. n. Kuri, 2007c) Sollte das doch der Fall sein, so Goll weiter, dann könne man diese Festplatte auch ohne Einsatz der Online-Durchsuchung beschlagnahmen und auswerten. Denn Terrorismus und Kinderpornografie ließen sich auch ohne Bundestrojaner wirkungsvoll bekämpfen. (vgl. Kuri, 2007c) Vorgehalten werden muss Goll allerdings, dass er das Problem der Verschlüsselung in der Tat übersieht<sup>35</sup>. Dennoch, Datenschützer befürchten, dass das BKA durch die heimlichen Überwachungsmaßnahmen zu einer Art „nationalen Superpolizeibehörde“ mutiert. Dramatisch drückte es die Abgeordnete Ulla Jelpke (Die Linke) aus:

*„Was da geschaffen wird, ist eine geheim ermittelnde Staatspolizei.“* (zit. n. Krempl & Briegleb, 2008c)

## 5 Exkurs Österreich

Anders als beim großen Nachbarn wurden in Österreich unter dem inzwischen vormaligen Innenminister Günther Platter, ohne größere Diskussionen oder Einmischung der Öffentlichkeit, vom Nationalrat das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert. Die neu erlangten Befugnisse der Polizei sollen zur Bekämpfung von Sexualstraftaten und Hooligan-Ausschreitungen eingesetzt werden. Ebenfalls im Gegensatz zur Bundesrepublik können die österreichischen Sicherheitsbehörden ohne richterlichen Vorbehalt auf die IMSI und Standortdaten von Mobilfunkteilnehmern zugreifen. Dies soll nur dann erlaubt sein, wenn „eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht“. Doch ob sich die Ermittlungsbehörden an diese Einschränkung wirklich gebunden fühlen, wird nicht von einer unabhängigen Kontrollinstanz überprüft. (vgl. Kuri, 2007e) Die Zahlen, die im Juni 2008 bekannt wurden, deuten unterdessen auf das Gegenteil hin. Auf Anfrage des Abgeordneten Alexander Zach (LiF) gab das Innenministerium zur Auskunft, dass von Jänner bis April in der gesamten Republik pro Tag rund 32 Internetuser überwacht wurden<sup>36</sup>. Insgesamt habe die Polizei zur Überwachung von Mobiltelefonen und Internetanschlüssen seit Inkrafttreten des neuen Sicherheitspolizeigesetzes (SPG) 3863 Anfragen gestellt, 258 davon bezogen sich auf Standorte und IMSI von Handys. (vgl. Winkler-Hermaden, 2008; Sokolov & Ziegler, 2008)

## 6 Gesellschaftliche Auswirkungen

*„On what grounds can we really charge someone who says: 'If surveillance doesn't really disturb me and if it helps to catch terrorists and child molesters and protect my credit card, I think it's ok'.“* (Gaycken, 2007)

### 6.1 Ende der Unschuldsvermutung?

Wie wir bereits bei den Beispielen zur Umsetzung in Kapitel 4 gesehen haben, sind die neuen technologischen

<sup>35</sup>Oder aber er hat sich auf das, in der Cybercrime Convention geforderte Recht bezogen, wonach Behörden die Kooperation des Datenträgerbesitzer bei der Entschlüsselung verlangen können sollen. (Siehe dazu Kapitel 3.3 auf Seite 11)

<sup>36</sup>Umgerechnet entspricht dies einer Abfrage alle 45 Minuten.

Instrumente im Kampf gegen den Terror oder andere schwere Straftaten nicht fehlerfrei. Und das nicht nur, weil es sich dabei um teilweise unausgereifte, schlecht konzipierte Konzepte handelt, sondern ganz einfach auch, weil sich so sehr auf deren Unfehlbarkeit verlassen wird. Dabei wird nämlich über eine bedeutende Quelle von Fehlern hinweggesehen, den Menschen, der sich der Instrumente bedient. Die Technik wird zudem als so sicher und unfehlbar angesehen, dass die Schlussfolgerungen, die sich durch ihre Anwendung ergeben, in den Augen der Ermittler einfach stimmen müssen und nicht mehr hinterfragt werden.

Auch verhalten sich Terroristen ihrem Wesen nach möglichst unauffällig und unverdächtig. Wenn dies der Fall ist, wenn ein jeder ein Terrorist sein könnte, dann ist der nächste logische Schritt, die ganze Bevölkerung unter Generalverdacht zu stellen. (Krempf, 2007c, S. 38) Das führt, wie wir im Zuge dieser Arbeit wiederholt gesehen haben, zu pauschalen Überwachungsmaßnahmen gegenüber 450 Millionen EU-Bürgern und noch vielen weiteren Menschen weltweit.

Darüber hinaus führt die nicht hinterfragte Methode oft zu einer Beweislastumkehr. Verdächtige Menschen müssen in der Zukunft wohl viel häufiger ihre Unschuld beweisen, weil die Schuld ja durch Vorratsdaten, biometrische Lesegeräte u.s.w bereits belegt wurde. (vgl. Larnhof, 2006, S. 62ff) Dass dies nicht bloß Hirngespinnste des Autors und der von ihm rezipierten Wissenschaftler sind, soll anhand drei kurzer Fallbeispiele veranschaulicht werden.

Der Jus-Student Herr Weber<sup>37</sup> wurde bezichtigt, Kinderpornografische Materialien im Internet verbreitet zu haben. Bei der Ermittlung wurde festgestellt, dass Herr Weber nach gültigem Recht einen Anonymisierungsdienst betrieben hatte. Auch wurde auf seinem Rechner keine Kinderpornografie gefunden, und somit konnte nicht bewiesen werden, dass er die Materialien persönlich verbreitet hatte. Nach zwei Monaten wurde das Strafverfahren gegen ihn eingestellt, jedoch wurde nicht spezifisch festgestellt, dass er unschuldig sei. Dies bedingt, dass ihm möglicherweise eine Eintragung „zur Gefahrenabwehr“ im Verfahrenszentralregister droht, auf deren Löschung er keinen Anspruch hätte. Da der Student Weber aber spezifisch den Beruf eines Juristen anstrebt, könnte dies möglicherweise erhebliche Nachteile für ihn bedeuten. Die Staatsanwaltschaft verweigert die Feststellung der Unschuldigkeit Webers damit, dass man die Person, die tatsächlich die Daten verbreitet habe nicht habe ermitteln können. Derweil sei man zu Gunsten Webers davon ausgegangen, dass tatsächlich nicht er, sondern eine dritte Person über den Anonymisierungsdienst die Daten zur Verfügung gestellt habe. (Weber, 2007, S. 20)

Ein ähnlicher Fall ergab sich im Februar 2008, als ein Universitätsprofessor feststellen musste, dass die Polizei seine Wohnung nach Kinderpornografie durchsucht und seine Rechner beschlagnahmt hatte. Ihm wurde vorgeworfen, im August 2007 kinderpornografische Videos in einer Tauschbörse zum Download angeboten zu haben. Die Polizei hatte zum damaligen Zeitpunkt, noch während die Verbindung aufrecht gehalten wurde, den entsprechenden Internetprovider ermitteln lassen, wer sich hinter der entdeckten IP-Adresse verbarg. Nachdem der Beschuldigte auf seiner Unschuld beharrte, und persönlich Kontakt mit dem Provider aufgenommen hatte, wurde nach einigen Tagen festgestellt, dass der Internetprovider die IP-Adresse dem falschen Kunden zugeordnet hatte. Der wirkliche Schuldige konnte, in Ermanglung einer, in diesem Fall nützlichen Vorratsdatenspeicherung, nicht mehr ermittelt werden. (vgl. Mansmann, 2008) Es handelt sich hierbei zwar um einen menschlichen, aber häufigen und unter Umständen fatalen Fehler. Denn bereits der ledigliche Verdacht auf Besitz von Kinderpornographie kann die private Existenz und berufliche Laufbahn von unschuldig Verdächtigten vernichten. „Gegenüber Ehepartnern, Verwandten, Freunden, Kollegen, Arbeitgebern oder Vermietern lässt sich die Unschuldsvermutung eben nicht erzwingen.“ (Mansmann, 2008)

*„Wenn Ihre Nachbarn erfahren, warum die Polizei Ihren Rechner mitgenommen hat, hilft auch kein anschließender Freispruch erster Klasse mehr, sondern nur noch der Umzug in eine andere Stadt.“* (Mansmann, 2007, S. 3)

<sup>37</sup>Der Betroffene hat diesen Artikel selbst in der Club-Zeitschrift des CCC, der „Datenschleuder“ veröffentlicht und seinen Namen verständlicherweise geändert.

Der Umgang der Geheimdienste, wie etwa die CIA, oder aber auch der UN mit Terrorverdächtigen ist höchst fragwürdig. Ein einmaliger, allenfalls vager Verdacht kann für eine Privatperson eine „zivile Todesstrafe“ bedeuten. Der italienische Geschäftsmann ägyptischer Herkunft, Youssef Nada, geriet 2003 auf die UN-Terrorliste. Die CENTRAL INTELLIGENCE AGENCY verdächtigte ihn, einer der Geldgeber der Attentäter des 11. September zu sein. Die Konten des Verdächtigten wurden gesperrt, seine Reisemöglichkeiten stark eingeschränkt, und das alles, ohne dass er sich zu den Vorwürfen hätte äußern können. (Wilkens, 2008)

## 6.2 Vertrauensverhältnisse in Gefahr

Anonymität ist ein notwendiges Teil im Puzzle der Demokratie. Freie Meinungsäußerung, Arztgeheimnis und andere Vertrauensverhältnisse bilden die Basis für liberale Gesellschaften. Mit Maßnahmen wie der Vorratsdatenspeicherung oder der Online-Durchsuchung werden genau diese Vertrauensverhältnisse aber gefährdet. Wer weiß, dass seine Verkehrsdaten aufgezeichnet werden, wird sich schwer tun, unbefangen zu kommunizieren. Journalisten zum Beispiel sind dazu verpflichtet, die Anonymität ihrer Informanten zu beschützen. Somit hat jeder Journalist auch etwas zu verbergen. Das allseits bekannte Argument, „wer nichts zu verbergen hat, hat auch nichts zu befürchten“, zieht also hier nicht. Die Recherchen eines Journalisten sollten keine Quellen für Ermittlungsarbeit sein, doch viele Journalisten befürchten, dass diese Gefahr besteht, sollte die Online-Durchsuchung bundesweit durchgesetzt werden. (vgl. Zörner, 2007)

Vertreter von Medienverbänden befürchteten schon vor Einführung der verdachtsunabhängigen Vorratsdatenspeicherung, dass diese einem ungeheuerlichen Angriff auf die Pressefreiheit den Weg bahnt. Die Kontakte der Journalisten stehen nun den Ermittlern unbeschränkt offen, dies ist in keinster Weise mit einer Demokratie vereinbar. (vgl. Krempl, 2007g, S. 85) Ein Bericht des NDR-Magazins ZAPP berichtet über die Verhältnisse in Belgien, wo es seit 2005 eine, von den Reportern treffend als „Datensammelwut“ bezeichnete, Art der Vorratsdatenspeicherung gibt. Investigativer Journalismus wird durch das wachsame Auge des Staates erschwert, wenn nicht sogar vereitelt, Informanten möchten nicht mehr angerufen werden, mühsam aufgebaute Vertrauensverhältnisse brechen auseinander, die Quellen der Journalisten versiegen. (vgl. Zapp, 2007)

Bei Ärzten ist die Lage besonders prekär, denn Gesundheit ist ein sensibles Thema, Interessant vor allem für Versicherungen und Arbeitgeber. Schon alleine die Tatsache, dass überhaupt eine Behandlungsverhältnis zwischen einem Patienten und seinem Arzt besteht, unterliegt der Schweigepflicht. (Larnhof, 2006, S. 50) Neben Journalisten und Ehepartner fallen auch Ärzte in der BRD nicht in die Kategorie der besonders schützenswerten Berufe<sup>38</sup>. (vgl. Krempl, 2007f, S. 53)

Auch das Verhältnis zwischen Staat und Bürger sieht der Vizepräsident des Landesverfassungsgerichts Mecklenburg-Vorpommern, Helmut Wolf, gefährdet. Durch die Überwachungsmaßnahmen, die er ohnehin für verfassungswidrig hält, entstehe „ein Klima von grundlegendem Unbehagen, Misstrauen und Angst [...]“ (Krempl, 2007b, S. 51) Laut einer repräsentativen Umfrage der GESELLSCHAFT FÜR SOZIALFORSCHUNG UND STATISTISCHE ANALYSE (Forsa) unter 1002 Bundesbürgern am 27. und 28. Mai 2008 würde die Mehrheit der Befragten (517 Personen) wegen der Vorratsdatenspeicherung „davon absehen, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigten.“ (akv, 2008) Mit den Plänen für den Einsatz der Online-Durchsuchung zeichnet sich laut Christoph Wegener von der Uni Bochum ein weiterer „großer Vertrauensverlust“ auch in die Polizei ab. (zit. n. Krempl & Ziegler, 2007a)

Peissl hat in diesem Sinne bereits 2002 vorausgesagt, dass die sicherheitspolitischen Überreaktionen nicht die erwarteten Effekte haben, sondern auf lange Zeit tiefgreifende Veränderungen in den jeweiligen Gesellschaften mit sich bringen werden. (vgl. Peissl, 2002, S. 1)

<sup>38</sup>Nur Geistliche (aber keine Imame), Strafverteidiger und Abgeordnete sollen besonders geschützt werden

### 6.3 Drang zur Konformität

*„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten ... Gemeinwesens ist.“* (BVerfGE, 65, 1 42f zit. n. Kleinert, 2007, S. 5)

Dieser Auszug aus dem sogenannten Volkszählungsurteil des Bundesverfassungsgericht von 1983 ist heute fast noch zutreffender als damals. Auch wenn Maßnahmen wie die Vorratsdatenspeicherung sich im Grunde auf die reinen Verbindungsdaten beschränken, so lässt sich doch auch schon aus diesen Informationen, welche Dienste eine Person in welcher Art und Weise in Anspruch nimmt, darauf schließen, welche politischen, ideologischen, finanziellen, sexuellen oder religiösen Interessen und Neigungen diese Person hat. (vgl. Kreml & Kuri, 2006c) Dabei ist das Recht auf Privatsphäre aber eine der treibendsten Kräfte unserer gesellschaftlichen Entwicklungen. Denn demokratisch-liberale Gesellschaften bauen auf dem Prinzip auf, dass Menschen selbstbewusst und autonom Entscheidungen treffen. (vgl. Peissl, 2002, S. 8) Menschen können ihr Verhalten nur dann effektiv, frei und kreativ erproben, wenn sie sich in ihrer Privatsphäre unverletzt fühlen. Die Privatsphäre ist deshalb auch der einzige „Ort“, an dem wir unabhängig von den Mächtigen oder Einflussreichen unserem Leben eine eigene Laufrichtung geben, und damit sogar unsere Gesellschaft ein Stück weit beeinflussen können. Nur wer für seine Handlungen nicht ständig verurteilt wird oder unter ihrem Misserfolg leiden muss, kann sich selbst erfahren, verändern, entfalten und ein starkes Selbstbewusstsein entwickeln. (vgl. Gaycken, 2007)

Mehr Überwachung bedeutet jedoch, dass eine große Anzahl an Menschen von einer vergleichsweise kleinen Elite auf ihre Konformität kontrolliert wird. Das führt nicht nur zu asymmetrischen Hierarchien und beeinflussten Gedankengängen, sondern auch zu konservativen, starren Gesellschaften. (vgl. Peissl, 2002, S. 2) Gesellschaftliche Entwicklung findet nämlich nur dort statt, wo etwas „Anderes“ versucht wird, wo revolutionäre Gedanken gesponnen und neue Lebensweisen erprobt werden. Jede neue Idee ist zu Beginn ungewöhnlich, abnorm, auffällig und mit den traditionellen Verhaltensweisen unkonform, aber dies bedeutet nicht, dass sie nicht vielleicht als bessere Idee empfunden, und sich allgemein durchsetzen wird. Nicht nur eine liberale Gesellschaft, sondern das Leben auf der ganzen Erde läuft seit Jahrtausenden nach diesem Prinzip ab.

### 6.4 Unzureichender Schutz vor Missbrauch

Gesetze zur Überwachung und Datenspeicherung sprießen zwar wie Pilze aus dem Boden, woran es jedoch mangelt, sind Grenzen und Kontrollen. Wo werden die erhobenen Daten gespeichert? Wer hat Zugriff auf sie? Wozu werden sie benutzt? Und es bedarf nicht nur Gesetzen, sondern auch deren aktiven Durchsetzung. Die Materie ist komplex und immer neue Warnungen vor Terroranschlägen werben um die Zustimmung der Bürger, doch die Gefahr des Missbrauchs ist zu hoch, als dass man die Kontrolle vernachlässigen könnte. BKA-Präsident Ziercke kündigte in diesem Zusammenhang z. B. an, man plane, „ein rein technisches Servicezentrum und ein Kompetenzzentrum von BKA, Bundespolizei und Nachrichtendiensten [...] [d]amit nicht jede Behörde für sich technisch aufrüsten muss“. (zit. n. Kreml & Briegleb, 2008a) Die Trennung zwischen Kompetenzen von Polizei und Geheimdienstlern werde dabei aber natürlich wie geboten strikt eingehalten. Doch wie glaubwürdig sind solche Aussagen wenn sie nicht einmal zu kontrollieren sind? Wer kontrolliert - wo die Daten für manche doch so leicht zugänglich sind - ob nicht mal eben jemand Informationen über einen unliebsamen Nachbarn oder Konkurrenten einholt? Wer garantiert, dass die Kommunikationsdaten der Bürger nicht zu einem späteren

Zeitpunkt zu einer falschen Verdächtigung führen oder sonstwie missbraucht werden?

Zwar haben die nationalen Regierungen sowie die EU-Kommission unentwegt beteuert, dass der Zugang zu den Vorratsdaten strengstens kontrolliert werden soll, erste Entwürfe für „eine Normierung der Vorhaltung von Verbindungs- und Standortdaten“ des Europäischen Instituts für Standards in der Telekommunikation (ETSI<sup>39</sup>) sehen dennoch vor, dass Sicherheitsbehörden, denen einmal Zugriff gewährt wurde, auch weiterhin unbeschränkten Zugriff auf die Vorratsdaten haben sollen. (vgl. Krempl, 2007g, S. 84) Die Konsequenzen sind beträchtlich: Unter den Vorratsdaten z.B. finden sich hoch sensible Informationen: Wer bei der Aids-Beratung oder bei Suchthilfestellen anruft, wer Informant für diesen Journalisten oder jenen Politiker ist, u.s.w. Würden diese Daten durch unzureichende Sicherung an die Öffentlichkeit geraten, es hätte für viele katastrophale Folgen. (vgl. Krempl, 2007a, S. 61)

Eine Überwachungsinfrastruktur, wie sie derzeit Europaweit aufgebaut wird, lässt sich nicht von vorneherein vor Missbrauch schützen. Die Infrastruktur ist theoretisch in der Lage, jedes Individuum, zu jeder Zeit, überall zu überwachen. Zu welchen sozialen Netzwerken man gehört, wo man sich aufhält, welche Gesinnungen man teilt, alles kann ausgeforscht werden.

Dass das noch nicht passiert, liegt nicht an technischen Beschränkungen, sondern an den ethischen Überzeugungen unserer Gesellschaft und den wenigen einschränkenden, geschriebenen und ungeschriebenen Regeln im Umgang mit solchen Technologien. Wenn die aktuellen Trends sich nicht umkehren, sondern immer mehr Grenzen wegfallen und immer neue, bessere Überwachungsmaßnahmen gesetzt werden, was wird dann ein autoritäres Regime davon abhalten, sich dieser Infrastruktur in vollen Zügen zu bedienen? (vgl. Gaycken, 2007) Oder mit den Worten Boaz Ganors:

*„In the worst case scenario this situation could cause the rise of a 'strong man', who will introduce an authoriatarian-dictatorial government, while promising to 'annihilate terrorism at any cost'.” (Ganor, 2006, S. 178)*

„Andererseits könnten gerade im Hinblick auf die Biometrie wieder Kontrollversuche an Bedeutung gewinnen, Menschen "lasterhaftes Verhalten" buchstäblich von der Nasenspitze abzulesen.” (Peter Strasser (Krempf & Kuri, 2006d)

Es gibt einige Vorschläge, wie Missbrauch zu verhindern ist. Etwa indem man statt einer verdachtsunabhängigen Speicherung (Data Retention) nur eine anlassbezogene Speicherung (Data Preservation) vorsieht. (vgl. Larnhof, 2006, S. 43) Das gleiche Konzept - unter der Bezeichnung „Quick Freeze“ - verfolgt auch ein Vorschlag von Contanze Kurz und dem ehemaligen Landesdatenschutzbeauftragten von Berlin, Hansjürgen Garstka. Sie wollen durchsetzen, dass die Zugangsanbieter erst dann Daten speichern, wenn bei einem konkreten Tatverdacht eine Behörde dies fordert. (vgl. Krempf & Kuri, 2007a) Sollte die Vorratsdatenspeicherung vom EuGH als ungültig erklärt werden, wären Anlass und Gelegenheit für einen solchen Schritt gegeben.

Eine weitere Möglichkeit erörtern Kwiatkowski *et al.* (vgl. 2006, S. 246). Mit Bezug auf Denmark und Fenstermacher plädieren sie dafür, Daten in zwei unterschiedliche Formen einzuteilen, nämlich Daten über den Status einer Person und Daten über deren Aktivitäten. Erst wenn auffällige Aktivitäten und somit ein ausreichend begründeter Verdacht vorliegen, soll ein „klug entworfenes Auswertungswerkzeug“ (Kwiatkowski *et al.*, 2006, S. 246) die betroffenen Personen herausfiltern. Eine Verfeinerung dieses Systems läge nach Meinung des Autors darin, diese getrennt aufbewahrten Daten nur in einer Richtung auflösbar zu machen. Das wäre zwar mit erheblichem technischen Aufwand verbunden, würde aber verhindern können, dass ein Mitarbeiter der Sicherheitsbehörden oder ein Eindringling mal eben so die Aktivitäten einer bestimmten Person einsehen könnte.

<sup>39</sup>European Telecommunications Standards Institute

## 7 Verhältnismäßig effektiv?

*"Ich habe manchmal den Eindruck, wir werden ähnlich stark überwacht wie seinerzeit die DDR-Bürger von der Stasi." (Karl Korinek, zit. n. Krempl & Kuhlmann, 2007)*

Letztlich stellt sich die Frage, sind die getroffenen Maßnahmen über die im Rahmen dieser Arbeit präsentierten Risiken, Gefahren und gesellschaftlichen Auswirkungen denn nun wirklich effektiv im Kampf gegen den Terrorismus oder eben auch schwere Verbrechen?

Zu einem Teil sind sie das ohne jeden Zweifel! Zumindest für die Vorratsdatenspeicherung und für die Online-Durchsuchung - sollte sie denn jemals rechtlich wie technisch durchführbar sein - gilt, dass die Instrumente eine beachtenswerte Waffe im Kampf gegen Verbrechen wie Betrug, Urheberrechtsverstöße oder Kinderpornografie darstellen. Aber es stellt sich vor allem in einer demokratischen Gesellschaft eben nicht nur die Frage nach der Effektivität. Ebenso, wenn nicht sogar noch wichtiger ist die Frage nach der Verhältnismäßigkeit der Maßnahmen. Stehen die Einschränkungen, die eine gesamte Gesellschaft hinnehmen muß überhaupt noch in einem vertretbaren Verhältnis zu den schlussendlich erzielten Erfolgen?

Denn die Einschränkungen ihrer Privatsphäre haben, wie wir nach den Erörterungen in dieser Arbeit feststellen müssen, hauptsächlich die „einfachen“<sup>40</sup> Leute zu tragen. Wer die Ressourcen, den Willen und die nötige Bildung dazu hat, so Peissl (vgl. 2002, S. 8), wird anonym bleiben können. Zu dieser Gruppe werden aller Wahrscheinlichkeit Kriminelle gehören, aber nicht unsere Eltern, Freunde oder Bekannten.

Eine Gefahr, die von der nahezu unkontrollierten „Wut“ nach Datenspeicherung - seien es Internet- oder biometrische Daten - ausgeht, ist nicht bloß, dass sie einzeln zum Missbrauch anstiften oder zu Konformitätsbestrebungen führen werden. Das wirklich gefährliche ist die Verschränkung all dieser Daten und all jener Technologien, die eine lückenlose Überwachung möglich machen. Doch wie dem Autor scheint, wird dieser Gesamtzusammenhang entweder nicht gesehen oder den Menschen absichtlich nicht vermittelt.

Die oben gestellte Frage nach Verhältnismäßigkeit berührt auch das Befinden der Menschen, die unter den Maßnahmen leiden. Patrick Breyer, der in der BRD in der vordersten Reihe gegen Überwachungsmaßnahmen kämpft, betont, dass der Sicherheitsstaat im Kern Unsicherheit schafft und sich Widerstand bildet, „[w]o den Menschen die Luft zum Atmen mit einem Vordringen der Staatsmacht in immer weitere private Bereiche genommen [...]“ wird. (Krempl & Kuri, 2007b)

*„Vieles von dem, was kulturell dynamisch ist, was unser Dasein beglückt und unsere Entwicklung befruchtet, erwächst aus Zuständen der Unsicherheit.“ (Trojanow, 2008)*

Wer frei und unbeschwert leben möchte, muss nach allem Anschein, so paradox dies auch klingen mag, auf Sicherheit verzichten.

**„It is not so much staying alive,  
it's staying human that's important.“**

George Orwell: 1984

<sup>40</sup>Der Begriff des „gemeinen“ Bürgers wäre an dieser Stelle wohl etwas zu zweideutig.

## Literatur

- (2008). (01.07.2008) Prozess gegen Data-Retention gestartet. <http://futurezone.orf.at/it/stories/289506/>.
- (2008). Forsa-Umfrage: Vorratsdatenspeicherung verhindert sensible Gespräche. <http://www.vorratsdatenspeicherung.de/content/view/228/55/lang,en/>.
- (2008). Maxtor STM3750330AS 750 GB. <http://www.alternate.at/html/productDetails.html?artno=AEBM04>.
- FRED ANDRESEN (2007). Fresche Lauscher. *Linux-Magazin* (8), 96–98.
- DANIEL BACHFELD (2007). (11.06.2007) Belgische ePässe ohne Autorisierung auslesbar. <http://www.heise.de/newsticker/meldung/90962>.
- PATRICK BATARILLO (2006). Daumen hoch für mehr Sicherheit. <http://www.ard.de/ratgeber/special/biometrischer-pass/-/id=322978/nid=322978/did=319952/z68vfz/index.html>.
- HENNING BEHME (2006). (11.10.2006) ePass birgt Sicherheitsrisiken. <http://www.heise.de/newsticker/ePass-birgt-Sicherheitsrisiken-/meldung/79292>.
- P. BIHR (2007). (20.07.2007) Online-Politik: Computerfreak als Lobbyist. <http://www.taz.de/1/archiv/dossiers/dossier-ueberwachung/online-durchsuchung/artikel/1/computerfreak-als-lobbyist-1/>.
- DANIELA M BÖCKLE (2004). *Datenschutz in Europa Unter Besonderer Berücksichtigung Des Datenschutzes Im Telekommunikationssektor*. Master's thesis, Innsbruck.
- DETLEF BORCHERS (2006). (11.12.2006) BGH verbietet Online-Durchsuchung von Computersystemen. <http://www.heise.de/newsticker/meldung/82341>.
- DETLEF BORCHERS & VOLKER BRIEGLEB (2007). (04.10.2007) Gutachter bezweifeln Durchführbarkeit von heimlichen Online-Durchsuchungen. <http://www.heise.de/newsticker/Gutachter-bezweifeln-Durchfuehrbarkeit-von-heimlichen-Online-Durchsuchungen-/meldung/96914/from/rss09>.
- DETLEF BORCHERS & VOLKER BRIEGLEB (2008). (18.06.2008) SPD will BKA-Gesetz korrigieren. <http://www.heise.de/newsticker/SPD-will-BKA-Gesetz-korrigieren-/meldung/109623>.
- DETLEF BORCHERS & JÜRGEN KURI (2007a). (05.02.2007) Schäuble heizt nach BGH-Urteil Debatte um Online-Durchsuchung an. <http://www.heise.de/newsticker/Schaeuble-heizt-nach-BGH-Urteil-Debatte-um-Online-Durchsuchung-an-/meldung/84813>.
- DETLEF BORCHERS & JÜRGEN KURI (2007b). (19.06.2007) Bundesregierung: Terroristen nutzten keine deutschen Pässe. <http://www.heise.de/newsticker/Bundesregierung-Terroristen-nutzten-keine-deutschen-Paesse-/meldung/91398>.
- DETLEF BORCHERS & JÜRGEN KURI (2007c). (25.07.2007) Online-Durchsuchung: Ist die Festplatte eine Wohnung? <http://www.heise.de/newsticker/Online-Durchsuchung-Ist-die-Festplatte-eine-Wohnung-/meldung/93307>.
- DETLEF BORCHERS & JÜRGEN KURI (2007d). (30.08.2007) Online-Durchsuchung: Mit Unikaten gegen Straftaten. <http://www.heise.de/newsticker/Online-Durchsuchung-Mit-Unikaten-gegen-Straftaten-/meldung/95200>.
- DETLEF BORCHERS & JÜRGEN KURI (2008). (30.01.2008) Europäischer Polizeikongress: Heimliche Online-Durchsuchung unverzichtbar. <http://www.heise.de/newsticker/Europaeischer-Polizeikongress-Heimliche-Online-Durchsuchung-unverzichtbar-/meldung/102700>.
- DETLEF BORCHERS & PETER-MICHAEL ZIEGLER (2007). (28.03.2007) ePässe bescheren Bundesdruckerei Umsatzrekord. <http://www.heise.de/newsticker/ePaesse-bescheren-Bundesdruckerei-Umsatzrekord-/meldung/87507>.
- JOHANN ČAS (2001). Cybercrime-Konvention des Europarates. <http://epub.oew.ac.at/ita/ita-newsletter/NL1201.pdf>.
- ALEX CONTE (2006). *The ICT Project on Human Rights Compliance when Countering Terrorism: A Guide to Legislators, Policy-Makers and Judges*, 279325. WBV, Bertelsmann, Bielefeld. ISBN 97615949X.

- EITEL DIGNATZ (2007). Irrlichternde Blicke. *Linux-Magazin* (07/07), 100.
- EUROPARAT (2001). Convention on Cybercrime. <http://www.interpol.int/Public/TechnologyCrime/Conferences/6thIntConf/>
- MARTIN FISCHER (2008). (10.06.2008) Zahl deutscher Internet-Nutzer wächst um fünf Prozent. <http://www.heise.de/newsticker/Zahl-deutscher-Internet-Nutzer-waechst-um-fuenf-Prozent-/meldung/109249>.
- LOTHAR GAMPER (2007). *Datenschutz Im Rahmen Der EMRK Am Beispiel Der Übermittlung Von Passagierdaten Im Flugverkehr an Zollbehörden Unter Berücksichtigung Europarechtlicher Aspekte*. Master's thesis, Innsbruck.
- BOAZ GANOR (2006). *Countering Terrorism. A challenge to Democracy*, 177–181. WBV, Bertelsmann, Bielefeld. ISBN 97615949X.
- SANDRO GAYCKEN (2007). Arguments Against Surveillance. 'Cos "I Don't Like It" Is Not Enough! <http://events.ccc.de/camp/2007/Fahrplan/events/2021.en.html>.
- JAN KLEINERT (2007). Was einstmals zählte. *Linux-Magazin* (05/07), 5.
- STEFAN KREMPL (2007a). Dammbbruch beim Datenschutz. Der Bundestag hat die Vorratsdatenspeicherung von Telefon- und Internetdaten abgesegnet. *c't - Magazin für Computertechnik* (25), 60f.
- STEFAN KREMPL (2007b). Daten auf Vorrat. Bundesrat billigt Gesetz zur Neuregelung der Telekommunikationsüberwachung (26/07).
- STEFAN KREMPL (2007c). Der Schäuble Katalog. Von der Anti-Terrordatei zum Präventivstaat. *c't - Magazin für Computertechnik* (09/07), 38–42.
- STEFAN KREMPL (2007d). Festplatte im Staatsvisier. Wie Wolfgang Schäuble PCs online durchsuchen lassen will. *c't - Magazin für Computertechnik* (20), 86–89.
- STEFAN KREMPL (2007e). Polizei ohne Grenzen. Datenbanken der EU-Strafverfolger werden vernetzt, Europol ausgebaut. *c't - Magazin für Computertechnik* (14/07), 50.
- STEFAN KREMPL (2007f). Unter Beobachtung. *c't - Magazin für Computertechnik* (10/07), 52f.
- STEFAN KREMPL (2007g). Wachsender Datenhunger unter Beschuss. 15.000 Demonstranten bekräftigten die breite Kritik am "Überwachungswahn". *c't - Magazin für Computertechnik* (22), 84–86.
- STEFAN KREMPL (2008). Hacker unter Volldampf. Trotz verlorener Schlachten an der Überwachungsfront: der CCC-Kongress im Zeichen des politischen Aktivismus. *c't - Magazin für Computertechnik* (02/08), 20,22,23.
- STEFAN KREMPL & VOLKER BRIEGLEB (2007a). (06.06.2007) Biometrische Personalausweise sollen über Brüssel kommen. <http://www.heise.de/newsticker/meldung/90754>.
- STEFAN KREMPL & VOLKER BRIEGLEB (2007b). (2.10.2007) "Feuchte Hände" vor Ausgabe der neuen Pässe mit Fingerabdrücken. <http://www.heise.de/newsticker/Feuchte-Haende-vor-Ausgabe-der-neuen-Paesse-mit-Fingerabdruecken-/meldung/96859>.
- STEFAN KREMPL & VOLKER BRIEGLEB (2007c). Mustermanns Fingerabdruck. Bundestag segnet Aufnahme von Fingerabdrücken in Reisepässen ab. *c't - Magazin für Computertechnik* (13), 41.
- STEFAN KREMPL & VOLKER BRIEGLEB (2008a). (02.06.2008) BKA will für Online-Razzien in die Wohnungen Verdächtiger. <http://www.heise.de/newsticker/BKA-will-fuer-Online-Razzien-in-die-Wohnungen-Verdaechtiger-/meldung/108847>.
- STEFAN KREMPL & VOLKER BRIEGLEB (2008b). (06.06.2008) Bayern will Onlinedurchsuchungen auch bei schweren Straftaten. <http://www.heise.de/newsticker/meldung/109118>.
- STEFAN KREMPL & VOLKER BRIEGLEB (2008c). (20.06.2008) Große Koalition verteidigt geplante Novelle des BKA-Gesetzes. <http://www.heise.de/newsticker/Grosse-Koalition-verteidigt-geplante-Novelle-des-BKA-Gesetzes-/meldung/109743>.
- STEFAN KREMPL & AXEL KOSSEL (2007). (30.09.2007) Schäuble: "Ich mache den Menschen gar keine Angst.". <http://www.heise.de/newsticker/Schaeuble-Ich-mache-den-Menschen-gar-keine-Angst-/meldung/96769/from/rss09>.

- STEFAN KREMPL & ULRIKE KUHLMANN (2007). (23.09.2007) Österreichs Verfassungsrichter warnt vor neuer Stasi. <http://www.heise.de/newsticker/Oesterreichs-Verfassungsrichter-warnt-vor-neuer-Stasi-/meldung/96393/from/rss09>.
- STEFAN KREMPL & JÜRGEN KURI (2006a). (01.06.2006) Irland und die Slowakei legen Klage gegen Vorratsdatenspeicherung ein. <http://www.heise.de/newsticker/Irland-und-die-Slowakei-legen-Klage-gegen-Vorratsdatenspeicherung-ein-/meldung/73751>.
- STEFAN KREMPL & JÜRGEN KURI (2006b). (01.12.2006) Bundestag verabschiedet neue Anti-Terrorgesetze. <http://www.heise.de/newsticker/Bundestag-verabschiedet-neue-Anti-Terrorgesetze-/meldung/81859>.
- STEFAN KREMPL & JÜRGEN KURI (2006c). (16.11.2006) Nutzerlobby gegen Lizenz zur "Dauerüberwachung" im Internet. <http://www.heise.de/newsticker/Nutzerlobby-gegen-Lizenz-zur-Dauerueberwachung-im-Internet-/meldung/81166>.
- STEFAN KREMPL & JÜRGEN KURI (2006d). (28.06.2006) CDU/CSU-Fraktion liebäugelt mit zentraler Speicherung biometrischer Daten. <http://www.heise.de/newsticker/CDU-CSU-Fraktion-liebaeugelt-mit-zentraler-Speicherung-biometrischer-Daten-/meldung/74796>.
- STEFAN KREMPL & JÜRGEN KURI (2007a). (17.09.2007) Generalbundesanwalt gegen "hysterisch gewordene Datenschutzdebatte". <http://www.heise.de/newsticker/Generalbundesanwalt-gegen-hysterisch-gewordene-Datenschutzdebatte-/meldung/96104>.
- STEFAN KREMPL & JÜRGEN KURI (2007b). (22.09.2007) Polizeizugriffe bei Demo gegen den Überwachungsstaat. <http://www.heise.de/newsticker/Polizeizugriffe-bei-Demo-gegen-den-Ueberwachungsstaat-/meldung/96388>.
- STEFAN KREMPL & JÜRGEN KURI (2007c). (31.10.2007) Bundesdruckerei zeigt sich gewappnet für neue Reisepässe. <http://www.heise.de/newsticker/Bundesdruckerei-zeigt-sich-gewappnet-fuer-neue-Reisepaesse-/meldung/98262>.
- STEFAN KREMPL & JÜRGEN KURI (2007d). Online-Zugriff auf Passbilder und Fingerabdrücke sorgt weiter für Wirbel. <http://www.heise.de/newsticker/Online-Zugriff-auf-Passbilder-und-Fingerabdruecke-sorgt-weiter-fuer-Wirbel-/meldung/88201>.
- STEFAN KREMPL & JÜRGEN KURI (2008a). (02.03.2008) BKA-Chef fordert Ende der Debatte über Online-Durchsuchungen. <http://www.heise.de/newsticker/BKA-Chef-fordert-Ende-der-Debatte-ueber-Online-Durchsuchungen-/meldung/104336>.
- STEFAN KREMPL & JÜRGEN KURI (2008b). (22.01.2008) Irland will dreijährige Vorratsdatenspeicherung per Verordnung erlassen. <http://www.heise.de/newsticker/Irland-will-dreijaehrige-Vorratsdatenspeicherung-per-Verordnung-erlassen-/meldung/102194>.
- STEFAN KREMPL & JÜRGEN KURI (2008c). (27.02.2008) Karlsruhe lässt kaum Raum für heimliche Online-Durchsuchungen. <http://www.heise.de/newsticker/Karlsruhe-laesst-kaum-Raum-fuer-heimliche-Online-Durchsuchungen-/meldung/104134>.
- STEFAN KREMPL & JÜRGEN KURI (2008d). (28.02.2008) Richter halten Kontrolle von heimlichen Online-Durchsuchungen für illusorisch. <http://www.heise.de/newsticker/Richter-halten-Kontrolle-von-heimlichen-Online-Durchsuchungen-fuer-illusorisch-/meldung/104238>.
- STEFAN KREMPL & AXEL VAHLDIK (2007). (16.09.2007) Mit dem Bundestrojaner gegen Anschläge mit schmutzigen Bomben. <http://www.heise.de/newsticker/Mit-dem-Bundestrojaner-gegen-Anschlaege-mit-schmutzigen-Bomben-/meldung/96055>.
- STEFAN KREMPL & ANDREAS WILKENS (2008a). (17.03.2008) Studie: Vorratsdatenspeicherung nutzt der Strafverfolgung kaum. <http://www.heise.de/newsticker/Studie-Vorratsdatenspeicherung-nutzt-der-Strafverfolgung-kaum-/meldung/105150>.
- STEFAN KREMPL & ANDREAS WILKENS (2008b). (19.03.2008) Bundesverfassungsgericht schränkt Vorratsdatenspeicherung ein. <http://www.heise.de/newsticker/Bundesverfassungsgericht-schraenkt-Vorratsdatenspeicherung-ein-/meldung/105284>.
- STEFAN KREMPL & PETER-MICHAEL ZIEGLER (2007a). (22.10.2007) Forscher fühlen sich in IT-Sicherheitsfragen vom Parlament "vergackeiert". <http://www.heise.de/newsticker/Forscher-fuehlen-sich-in-IT-Sicherheitsfragen-vom-Parlament-vergackeiert-/meldung/97771>.

- STEFAN KREMPL & PETER-MICHAEL ZIEGLER (2007b). (23.04.2007) Expertenstreit über Fingerabdrücke in Pässen. <http://www.heise.de/newsticker/Expertenstreit-ueber-Fingerabdrucke-in-Paessen-/meldung/88704/from/rss09>.
- STEFAN KREMPL & PETER-MICHAEL ZIEGLER (2008a). (03.01.2008) EU-Kommission pocht auf Umsetzung der Vorratsdatenspeicherung. <http://www.heise.de/newsticker/EU-Kommission-pocht-auf-Umsetzung-der-Vorratsdatenspeicherung-/meldung/101268>.
- STEFAN KREMPL & PETER-MICHAEL ZIEGLER (2008b). (21.04.2008) Abhören von Internet-Telefonie als Einfallstor für den Bundestrojaner? <http://www.heise.de/newsticker/Abhoeren-von-Internet-Telefonie-als-Einfallstor-fuer-den-Bundestrojaner-/meldung/106793>.
- JÜRGEN KURI (2007a). (06.02.2007) BKA-Chef hält Online-Durchsuchungen für dringend erforderlich. <http://www.heise.de/newsticker/BKA-Chef-haelt-Online-Durchsuchungen-fuer-dringend-erforderlich-/meldung/84843>.
- JÜRGEN KURI (2007b). Alarmstufe. Terrorverdacht heizt Debatte um Online-Durchsuchung an. *c't - Magazin für Computertechnik* (20), 43.
- JÜRGEN KURI (2007c). Bayern will Regelung zu Online-Durchsuchungen vorantreiben. <http://www.heise.de/newsticker/Bayern-will-Regelung-zu-Online-Durchsuchungen-vorantreiben-/meldung/84864>.
- JÜRGEN KURI (2007d). Heimliche Online-Durchsuchungen sind unzulässig. <http://www.heise.de/newsticker/Heimliche-Online-Durchsuchungen-sind-unzulaessig-/meldung/84776>.
- JÜRGEN KURI (2007e). Überwachung: Neuer Streit in Deutschland, neue Recht für Österreichs Polizei. *c't - Magazin für Computertechnik* (01/08), 26.
- JÜRGEN KURI (2008). (27.05.2008) Kriminalbeamte fordern zentrale Datenbank für Verbindungsdaten. <http://www.heise.de/newsticker/Kriminalbeamte-fordern-zentrale-Datenbank-fuer-Verbindungsdaten-/meldung/108497>.
- MELANIE KWIATKOWSKI, STEFANIE HÖHFELD & INA KRADEPOHL (2006). *Der Einsatz von Ontologien bei Retrieval-Systemen von Intelligence Services - am Beispiel von Convera RetrievalWare -*, 243–265. WBV, Bertelsmann, Bielefeld. ISBN 97615949X.
- ODA LAMBRECHT (2005). Sehnen nach Sicherheit. <http://www.ard.de/ratgeber/special/terrorismus/-/id=322978/nid=322978/did=319878/1c8zypw/index.html>.
- KARIN LARNHOF (2006). *Data Retention. Zur aktuellen Rechtslage in einigen ausgewählten EU-Mitgliedsländern unter Berücksichtigung der EU-Richtlinie zur Vorratsdatenspeicherung*. Master's thesis, Fachhochschule Eisenstadt.
- JOHN LETTICE (2006). How to clone the copy-friendly biometric passport. [http://www.theregister.co.uk/2006/08/04/cloning\\_epassports/](http://www.theregister.co.uk/2006/08/04/cloning_epassports/).
- HARTMUT LUBOMIERSKI (2006). 20. Tätigkeitsbericht des Hamburgischen Datenschutzauftragten zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht öffentlichen Bereich 2004 / 2005. <http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzauftragter/taetigkeitsberichte/taetigkeitsbericht-20-jahr-2004-2005-pdf,property=source.pdf>.
- NILS MAGNUS (2007). Einbruch für den Bund. Zehn Einfallstore für einen Linux-Bundestrojaner und zehn Abwehrstrategien. *Linux-Magazin* (11/07), 102–107.
- URS MANSMANN (2007). Die totale Verdattung. *c't - Magazin für Computertechnik* (10/07), 3.
- URS MANSMANN (2008). Unschuldig unter Verdacht. DSL-Provider meldete falsche Kundenadresse ans BKA. *c't - Magazin für Computertechnik* (08/08), 39.
- PETER MUEHLBAUER (2008). (06.01.2008) Schäuble sieht Gewaltkriminalität als Argument für Vorratsdatenspeicherung. <http://www.heise.de/newsticker/meldung/101345>.

- HEINRICH NEISSER (2006). *Datenschutzentwicklung in der Europäischen Union*, 327–340. WBV, Bertelsmann, Bielefeld. ISBN 97615949X.
- WALTER PEISSL (2001). Überwachung und Sicherheit - Grundrechte in Gefahr. <http://epub.oeaw.ac.at/ita/ita-newsletter/NL1201.pdf>.
- WALTER PEISSL (2002). Surveillance and Security - A Dodgy Relationship. [http://www.oeaw.ac.at/ita/pdf/ita\\_02\\_02.pdf](http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf).
- CHRISTIAN RATH (2007). (08.02.2007) "Terroristen sind auch klug" - Interview mit Bundesinnenminister Wolfgang Schäuble. <http://www.taz.de/index.php?id=archivseite&dig=2007/02/08/a0169>.
- CHRISTIAN RATH (2008). Regierung einigt sich bei Schnüffelei. <http://www.taz.de/1/archiv/dossiers/dossier-ueberwachung/online-durchsuchung/artikel/1/zypries-und-schaeuble-einig-bei-schnueffelei/>.
- FRANK ROSENGART (2005). Biometrische Verfahren in der Praxis ungeeignet. <http://www.ccc.de/epass/biopii?language=de>.
- CHRISTIANE RÜTTEN (2006). (02.02.2006) ePass-Hack im niederländischen TV demonstriert. <http://www.heise.de/newsticker/ePass-Hack-im-niederlaendischen-TV-demonstriert-/meldung/69127>.
- DANIEL SCHULZ (2008). (30.05.2008) Wenn abgeschnittene Finger Zugang schaffen: Die blutigen Folgen der Biometrie. <http://www.taz.de/1/archiv/dossiers/dossier-ueberwachung/biometrie/artikel/1/die-blutigen-folgen-der-biometrie/>.
- DANIEL SOKOLOV & PETER-MICHAEL ZIEGLER (2008). (26.06.2008) Österreichs Polizei nutzt neue Überwachungsrechte intensiv. <http://www.heise.de/newsticker/Oesterreichs-Polizei-nutzt-neue-Ueberwachungsrechte-intensiv-/meldung/110080>.
- MARC STÖRING (2008). Umstrittene Einblicke. Staatliche E-Mail-Überwachung auf unklarer Rechtsgrundlage. *c't - Magazin für Computertechnik* (14/08), 156,158.
- ILIJA TROJANOW (2008). Mit Sicherheit untergehen. <http://derstandard.at/?url=/?id=3265402>.
- KARSTEN UMLAUF (2006). Datensammler gegen Bürgerrechtler. Die Parteien zum Datenschutz. <http://www.ard.de/ratgeber/special/parteien-zum-datenschutz/-/id=322978/nid=322978/did=319908/1r3fz3o/index.html>.
- HERR WEBER (2007). Anonymisierungsdienst TOR: Wenn die Polizei 2x klingelt. *Datenschleuder* (91), 16–20.
- ANDREAS WILKENS (2007). (12.04.2007) Polizei soll automatisch auf digitale Passfotos zugreifen können. <http://www.heise.de/newsticker/Polizei-soll-automatisch-auf-digitale-Passfotos-zugreifen-koennen-/meldung/88126>.
- ANDREAS WILKENS (2008). (23.01.2008) Europarat fordert Rechte für Terrorverdächtige. <http://www.heise.de/newsticker/Europarat-fordert-Rechte-fuer-Terrorverdaechtige-/meldung/102308>.
- ROSA WINKLER-HERMADEN (2008). 32 User pro Tag überwacht. *Der Standard* 6.
- ZAPP (2007). Protest - Journalisten kämpfen gegen Überwachung. [http://www3.ndr.de/ndrtv\\_pages\\_video/0,,OID4287466\\_VID4286362,00.html](http://www3.ndr.de/ndrtv_pages_video/0,,OID4287466_VID4286362,00.html).
- PETER-MICHAEL ZIEGLER (2006). Sicherheitsexperte führt Klonen von RFID-Reisepässen vor. <http://www.heise.de/newsticker/Sicherheitsexperte-fuehrt-Klonen-von-RFID-Reisepaessen-vor-/meldung/76379>.
- PETER-MICHAEL ZIEGLER (2008). (09.01.2008) CSU will Bundestrojaner auch gegen Kinderpornographie einsetzen. <http://www.heise.de/newsticker/CSU-will-Bundestrojaner-auch-gegen-Kinderpornographie-einsetzen-/meldung/101537>.
- HENDRIK ZÖRNER (2007). Informantenschutz in Gefahr. <http://www.taz.de/1/archiv/dossiers/dossier-ueberwachung/online-durchsuchung/artikel/1/wir-haben-alle-etwas-zu-verbergen/>.