

Jahr: 2010
Autor: Moritz Tremmel
Web: moritztremmel.de
Lizenz: Creative Commons (BY)
<http://creativecommons.org/licenses/by/3.0/de/deed.de>

Die Vorratsdatenspeicherung und der Panoptismus

**Anwendbarkeit und Erkenntnisse aus der Analyse
der Vorratsdatenspeicherung mit Foucaults
Machttheorie**

Inhaltsverzeichnis

1. Einleitung	1
2. Die Vorratsdatenspeicherung	4
2.1 Was bedeutet Vorratsdatenspeicherung?	4
2.2 Historie	4
2.2.1 Die Vorratsdatenspeicherung in der EU	4
2.2.2 Die Vorratsdatenspeicherung in Deutschland	5
2.2.3 Die Bundesverfassungsgerichtsentscheidung	6
2.2.4 Ein Blick in die Zukunft	6
3. Foucaults Machttheorie	8
3.1 Foucaults Machtbegrifflichkeiten	8
3.2 Die Disziplinarmacht	9
3.3 Der Panoptismus	10
3.3.1 Die Architektur	10
3.3.2 Die Wirkungsweise	10
3.3.3 Das panoptische Prinzip	11
4. Analyse	12
4.1 Anwendbarkeit des panoptischen Prinzips	12
4.1.1 Vielzahl von Individuen	12
4.1.2 Aufzwingen eines Verhaltens oder einer Aufgabe	12
4.2 Asymmetrie durch die Maschinerie des Panoptikums	13
4.3 Trennung von sehen und gesehen werden	14
4.3.1 Uneinsehbarkeit der Überwachung	14
4.3.2 Sichtbarkeit der Überwachten	16
a) Extraktion von Wissen aus den Verkehrsdaten	16
b) Beschränkungen beim Abruf der Daten	18
c) Umgehung der Vorratsdatenspeicherung	19
d) Sichtbarkeit und Überprüfung der Konformität	20
4.4 Die bewusste Überwachung	21
4.5 Kontinuität der Überwachungswirkung	23
4.5.1 Permanente Überwachung	23

4.5.2 Verhaltensanpassung und -änderung	24
4.5.3 Kontinuierliche Wirkung der Überwachung	25
5. Fazit	26
5.1 Zusammenfassung der Untersuchung	26
5.2 Ergebnis der Analyse	28
5.3 Bewertung der Methode	28
5.4 Schlussfolgerungen	29
6. Quellen	30

I believe there is something out there watching us.
Unfortunately, it's the government.
Woody Allen

1. Einleitung

Ende 2007 waren auf etlichen Webseiten Todesanzeigen zu finden, manchmal findet man sie heute noch im Internet: „Das Fernmeldegeheimnis ist unverletzlich. 1949 – 2007 † SPD, CDU, CSU haben es beschlossen: Gläsernes Telefon, Handy und Internet *9.11.2007“¹. Parallel dazu stemmte die Netzgemeinde die größte Verfassungsbeschwerde in der deutschen Geschichte mit knapp 35'000 Beschwerdeführern.² Die Kläger fürchten nicht weniger als den Überwachungsstaat. Die Speicherung der Verkehrsdaten ermögliche die minutiöse Nachverfolgung der Leben der Betroffenen.

Gleichzeitig betonen Politiker aus dem Umfeld der Sicherheitsbehörden den massiven Sicherheitszugewinn durch die Vorratsdatenspeicherung (VDS). Der Internetkriminalität sowie dem internationalen Terrorismus sei ohne die Maßnahme kaum noch zu begegnen. Die rechtschaffenen Bürger bräuchten sich dabei aber keine Sorgen um ihre Daten zu machen, vielmehr sollten sie sich sicherer fühlen – letzten Endes würde die Vorratsdatenspeicherung die Freiheit schützen.

Zwei Seiten einer Medaille? Beide Kontrahenten bestreiten die Aussagen und Argumente des jeweils Anderen. Die Daten würden nicht vor dem internationalen Terrorismus schützen und Kinderpornographie würden sie ebenso wenig verhindern, betonen die Gegner. Vielmehr würden die herkömmlichen Ermittlungswerkzeuge ausreichen ohne die Grundrechte von Millionen Menschen auszuhöhlen. Das BKA hält dem entgegen, dass eine effektive Verbrechensbekämpfung ohne die Vorratsdatenspeicherung nicht möglich sei und die Daten für den Bürger keine negativen Auswirkungen haben würde – solange er sich nichts zu schulden kommen lasse.

1 AK Vorratsdatenspeicherung (2007)

2 Heise Online (2010c)

Am 2. März 2010, hat das Bundesverfassungsgericht das Gesetz zur Vorratsdatenspeicherung in Deutschland für nichtig erklärt, dennoch hielt es die Vorratsdatenspeicherung an sich nicht für verfassungswidrig; Vielmehr hat es nur die bisherige Umsetzung der EU-Richtlinie kritisiert, es erläutert aber gleichzeitig in seinem Urteil die Vorgaben für eine verfassungsgemäße Umsetzung.³ Dies macht Arbeiten wie die Folgende um so dringlicher. Auf den Erfahrungen der bisherigen Vorratsdatenspeicherung kann so eine Analyse der Machtwirkungen aufbauen, welche zudem die Diskussions- und Wissensbasis für den zukünftigen Umgang mit der Speicherung von Kommunikationsdaten auf Vorrat liefern sollte.

Die vorliegende Arbeit dient zum Einen der Analyse der Vorratsdatenspeicherung und der Darstellung ihrer Machtwirkungen anhand der Kriterien der foucaultschen Machttheorie, zum Anderen der Prüfung der Anwendbarkeit der foucaultschen Theorie auf eine komplex-abstrakte Überwachungstechnik.

Eine wissenschaftliche Untersuchung der Machtwirkung der Vorratsdatenspeicherung halte ich insbesondere in dem von Polemie durchdrungenen Feld der Überwachung für wichtig. Schnell wird mit der sexuellen Misshandlung von Kindern und blutigen Terroranschlägen argumentiert oder der jegliche Freiheit raubende Überwachungsstaat ins Feld geführt. Welche Wirkungen die konkrete Überwachungsmaßnahme auf die Menschen oder eine Gesellschaft hat, oder haben kann, bleibt dabei allzu oft außen vor. Zu der Vorratsdatenspeicherung existieren bisher nur wenige Studien, im speziellen, wenn es um die Wirkung und Entfaltung der Macht geht.⁴ Diesen Raum ein wenig zu füllen soll auch Aufgabe der vorliegenden Arbeit sein.

Zu Beginn meiner Arbeit werde ich einen historischen Abriss über die Implementierung der Vorratsdatenspeicherung auf EU- und Bundesebene liefern, die aktuelle Entscheidung des Bundesverfassungsgerichts thematisieren sowie einen kurzen Blick in die Zukunft wagen. Danach stelle ich die Machttheorie Foucaults vor. Hier werde ich mich im speziellen auf die überwachungsrelevanten Theorieteile wie das panoptische Prinzip⁵ konzentrieren. Daraufhin werde ich die Analyse der Vorratsdatenspeicherung

3 Bundesverfassungsgericht (2010)

4 Albrecht, Hans-Jörg (2008): S. 137 - 139

5 Der Soziologe Haggerty sieht dieses als das führende Wissenschaftsmodell für die Analyse von Überwachungssystemen an.
Haggerty, Kevin D. (2006): S. 23

mit den Werkzeugen Foucaults beginnen. Am Ende werde ich meine Ergebnisse zusammenfassen und ein Fazit aus der Arbeit ziehen.

Als Quellen ziehe ich dafür vor allem Studien und Stellungnahmen heran. Des Weiteren stütze ich mich auf Artikel aus der Fachliteratur sowie zur Thematik passenden Internetseiten. Als besonders wichtige Quelle ist das Bundesverfassungsgericht hervorzuheben, welches durch seine Einschränkungen sowie das Urteil selbst die Vorratsdatenspeicherung mitgestaltet hat. Ich analysiere die Vorratsdatenspeicherung auch im Hinblick auf die einstweilige Anordnung vom März 2008 sowie das Urteil vom März 2010. Diese bestimmen die reale bzw. zukünftige Ausgestaltung der Vorratsdatenspeicherung.

Die wichtigsten Studien bei der Analyse stellen die vom Max Planck Institut bzw. aus dessen Umfeld stammenden Studien zur Rechtswirklichkeit der Vorratsdatenspeicherung dar. Des Weiteren stütze ich mich an mehreren Punkten auf eine repräsentative Forsa-Umfrage.

Neben den Studien spielen die Stellungnahmen die an das Bundesverfassungsgericht übersandt wurden eine bedeutende Rolle. Der Datenschutzbeauftragte Peter Schaar sowie der Chaos Computer Club konnten anhand ihrer Weitsicht und ihres Fachwissens überzeugen – auch das Bundesverfassungsgericht griff auf diese als Experten zurück.

2. Die Vorratsdatenspeicherung

2.1 Was bedeutet Vorratsdatenspeicherung?

Vorratsdatenspeicherung bezeichnet die verdachtsunabhängige Speicherung der Verkehrs- und Kommunikationsdaten die durch Telekommunikation entstehen. Gemeint ist die Speicherung von jeglichen Daten die beispielsweise bei einem Telefonanruf, einer E-Mail oder einer SMS entstehen auf Vorrat (über einen längeren Zeitraum). Bei Handytelefonaten werden dabei zudem die Standorte gespeichert. Bei Internetanschlüssen die IP-Adresse⁶, die dem Nutzer zugeteilt wurde. Es werden auch Telekommunikationsversuche gespeichert. Der Inhalt der Kommunikation wird dabei nicht gespeichert.⁷

2.2 Historie

2.2.1 Die Vorratsdatenspeicherung in der EU

Am 15. März 2006 wurde die Richtlinie zur Einführung einer europaweiten Vorratsspeicherung von Telefon- und Internetdaten (Richtlinie 2006/24/EG) nach dem schnellsten Gesetzgebungsverfahren der EU-Geschichte verabschiedet. Ziel war es nach den Anschlägen in Madrid 2004 und London 2005 Möglichkeiten zur Bekämpfung des internationalen Terrorismus sowie der organisierten Kriminalität zu schaffen. Die Speicherung von Vorratsdaten sollte einheitlich stattfinden, um mit der gestiegenen mobilen Kommunikation und Internationalisierung Schritt halten zu können.⁸

Die Richtlinie sieht vor die Verkehrsdaten zwischen 6 und 24 Monate⁹ von Telekommunikationsanbietern speichern zu lassen. „Gespeichert werden sollen die Daten von Festnetz und Mobilfunk, von SMS, EMS und MMS und Internetprotokollen, nicht aber die Inhalte der jeweiligen Kommunikation.“¹⁰ Der Zugriff auf diese Daten ist auf 'schwere Straftaten' beschränkt, welche von den Mitgliedsstaaten unterschiedlich definiert werden.¹¹

6 Eine IP-Adresse ist eine Kennung aus dem Computerbereich. Sie wird im Internet vergeben um Internetanschlüsse eindeutig identifizieren und ansprechen zu können.

7 Engling, Dirk (2008): S. 68

8 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Alvaro, Alexander (2006): S. 52 - 54

9 Ein Mitgliedsstaat kann nach Begründung den Zeitraum allerdings nach oben hin verlängern.

10 Alvaro, Alexander (2006): S. 53

11 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

In Rumänien und Bulgarien wurden die dortigen Umsetzungen der Vorratsdatenspeicherung für verfassungswidrig erklärt.¹² Auch in einigen weiteren EU-Mitgliedsstaaten wurde die Vorratsdatenspeicherung bisher noch nicht umgesetzt (z.B. Schweden).¹³

2.2.2 Die Vorratsdatenspeicherung in Deutschland

Der Deutsche Bundestag lehnte die Speicherung von Verkehrsdaten schon mehrfach ab – u.a. 2004 bei der Revision des Telekommunikationsgesetzes.¹⁴ Eine Auskunftserteilung, über bei den Telekommunikationsanbietern zu Abrechnungszwecken gespeicherten Verbindungsdaten,¹⁵ ist jedoch schon seit dem 1. Januar 2002 möglich.¹⁶

Auf EU-Ebene wurde aber dennoch eine Vereinheitlichung der Speicherung der Kommunikationsverkehrsdaten diskutiert und eine Richtlinie beschlossen (siehe Punkt 2.2.1). EU-Richtlinien müssen in den Mitgliedsstaaten in nationale Gesetze umgesetzt werden. Die in der Bundesrepublik unpopuläre Vorratsdatenspeicherung kam so durch die europäische Hintertür nach Deutschland und trat zum 1. Januar 2008 in Kraft (mit einer Übergangsfrist bis 1. Januar 2009 für Internetdienstleister).¹⁷

Die Verwendbarkeit der Daten ging in Deutschland allerdings über die Vorgaben der EU deutlich hinaus. Die Daten der Vorratsdatenspeicherung durften auch zur Verfolgung von Straftaten im Allgemeinen, der Abwehr von erheblichen Gefahren für die öffentliche Sicherheit, zur Erfüllung von Geheimdienstaufgaben und bei Internetvergehen verwendet werden.

Für all diese Verwendungsmöglichkeiten galt eine weitere deutsche Besonderheit, der Richtervorbehalt. Ausgenommen hiervon war die Abfrage einer Identität, die hinter einer IP-Adresse steht.¹⁸

Alvaro, Alexander (2006): S. 52 -54

12 Heise Online (2009)

13 Krempf, Stefan (2010a)

14 Engling, Dirk (2008): S. 69

15 Sollten die Daten allerdings nicht benötigt werden (z.B. bei Flatrates) sind sie unverzüglich zu löschen. Es ist allerdings möglich die Daten dennoch einen gewissen Zeitraum zur Gefahrenabwehr zu speichern – so speichert die Telekom IP-Adressen bis zu 7 Tage.

16 Grafe, Adina (2007): S. 7

17 Engling, Dirk (2008): 69 - 71

18 Bundesgesetzblatt (2007): S. 3208
Bundesverfassungsgericht (2010)

Diese breite Verwendungsmöglichkeit, die deutlich über die von der EU-Richtlinie vorgesehenen 'schweren Straftaten' hinausgeht, wurde vom Bundesverfassungsgericht am 11. März 2008 aufgrund einer einstweiligen Anordnung auf 'schwere Straftaten', die sogenannten Katalogstraftaten, eingeschränkt.¹⁹

2.2.3 Die Bundesverfassungsgerichtsentscheidung

Das Bundesverfassungsgericht erklärt die deutsche Umsetzung der Vorratsdatenspeicherung am 2. März 2010 für nichtig. Sie sei nicht mit dem Grundgesetz (Art. 10 Abs. 1 GG – Telekommunikationsgeheimnis) vereinbar, die bisher gespeicherten Daten seien unverzüglich zu löschen. Der Grund dafür liegt in dem Fehlen des Verhältnismäßigkeitsgrundsatzes, es wäre „weder eine hinreichende Datensicherheit, noch eine hinreichende Begrenzung der Verwendungszwecke der Daten“²⁰ gegeben.

Eine Vorratsdatenspeicherung wurde allerdings nicht für unmöglich erklärt, vielmehr sei die Umsetzung der Richtlinie nicht Verfassungskonform – die Richtlinie selbst könne im Einklang mit dem Grundgesetz umgesetzt werden. Das Bundesverfassungsgericht nennt in seiner Entscheidung die Kriterien für eine konforme Umsetzung.²¹

2.2.4 Ein Blick in die Zukunft

Nach dem Urteil des Bundesverfassungsgerichts drängen Polizeiverbände, Polizisten, CDU/CSU sowie Vertreter des Innenministeriums auf eine Rasche Erneuerung der Vorratsdatenspeicherung unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts. Sie argumentieren dabei recht polemisch mit der angeblich unmöglich gewordenen Aufklärung von Straftaten im Internet, sowie Verbrechen der organisierten Kriminalität.²²

Als Reaktion darauf starten Bürgerrechtler eine Kampagne gegen eine Wiedereinführung der Vorratsdatenspeicherung in Deutschland. In einem offenen Brief wandten sich 48 Organisationen, vor allem aus der Zivilgesellschaft, darunter Reporter

19 Deutscher Bundestag (2008): S. 1 - 3

20 Bundesverfassungsgericht (2010)

21 Bundesverfassungsgericht (2010)

22 Heise Online (2010d)

ohne Grenzen, die Bundesarbeitsgemeinschaft Kritischer Polizistinnen und Polizisten und die Deutsche AIDS-Hilfe, an die Bundesjustizministerin. Diese solle sich gegen eine Wiedereinführung stark machen und sich für eine vollständige Abschaffung der Richtlinie auf EU-Ebene einsetzen. Die Vorratsdatenspeicherung behindere die Kommunikationsfreiheit unzumutbar und setze vertrauliche Tätigkeiten und Kontakte etwa zu Journalisten, Beratungsstellen und Geschäftspartnern dem ständigen Risiko eines Bekanntwerdens aus.²³

Die Kontrahenten können jeweils einen zuständigen Minister auf ihrer Seite wissen. Der Innenminister De Maizière fordert das Urteil zügig und klug umzusetzen. Die Justizministerin Leutheusser-Schnarrenberger hält die Vorratsdatenspeicherung für verzichtbar und möchte das Urteil in Ruhe auswerten und auch über Alternativen wie das Quick-Freeze-Verfahren nachdenken. Bei diesem werden die vorliegenden Telekommunikationsdaten, bei Verdacht eingefroren, ohne anlasslos die Daten aller Kommunikationsteilnehmer zu speichern.²⁴

Auch auf EU-Ebene wird über die Vorratsdatenspeicherung diskutiert. EU-Justizkommissarin und Vizepräsidentin der Kommission Viviane Reding kündigte im Februar an die Richtlinie „noch in diesem Jahr auf den Prüfstand zu stellen“.²⁵ EU-Innenkommissarin Cecilia Malmström will die EU-Richtlinie bis Ende des Jahres evaluieren lassen. Zu prüfen sei ob die Speicherung der Vorratsdaten angemessen und effektiv sei, aber auch ob sie mit der Grundrechtecharta des Lissabon-Vertrags, welche Ende 2009 in Kraft getreten ist, vereinbar sei.²⁶

Eine zuverlässige Prognose wie die 'Schlacht um die Vorratsdatenspeicherung' ausgehen wird, ist momentan unmöglich. Umso wichtiger ist eine Erforschung der Wirkung der Vorratsdatenspeicherung.

23 Heise Online (2010c)

Kremp, Stefan (2010)

24 Kremp, Stefan (2010b)

25 Heise Online (2010b)

26 Heise Online (2010a)

3. Foucaults Machttheorie

Zur Analyse der Vorratsdatenspeicherung ziehe ich die Machttheorie von Foucault heran. Dieser arbeitete Zeit seines akademischen Lebens an seiner Machttheorie – er sah sich dabei als Experimentator, der seine Gedanken kontinuierlich weiterentwickelt und verändert. Foucault liefert dabei nicht eine Theorie im systemischen oder ideologischen Sinne, vielmehr bietet Foucault eine Werkzeugkiste.²⁷

Ich beziehe mich in meiner Analyse der Vorratsdatenspeicherung vor allem auf die in »Überwachen und Strafen« entwickelten Machtbegrifflichkeiten. Das Buch thematisiert, wie der Titel schon andeutet, Überwachungsmaßnahmen und ist damit besonders für die Analyse der Vorratsdatenspeicherung geeignet. Die Hauptkonzepte hierfür sind die Disziplinarmacht und der darauf basierende Panoptismus. Diese werde ich im Folgenden vorstellen.

3.1 Foucaults Machtbegrifflichkeiten

Foucault verlagert mit seiner Analyse der Macht die Perspektive. Macht ist nicht, wie beispielsweise bei Weber, die Chance eines Subjekts sich gegenüber anderen durchzusetzen, vielmehr stellt Foucault auf die Prozesshaftigkeit von Machtausübungen und -wirkungen ab.²⁸

„Diese Macht ist nicht so sehr etwas, was jemand besitzt, sondern vielmehr etwas, was sich entfaltet; nicht so sehr das erworbene oder bewahrte »Privileg« der herrschenden Klasse, sondern vielmehr die Gesamtwirkung ihrer strategischen Positionen – eine Wirkung, welche durch die Position der Beherrschten offenbart und gelegentlich erneuert wird. Ander[er]seits richtet sich diese Macht nicht einfach als Verpflichtung oder Verbot an diejenigen, welche »sie nicht haben«; sie sind ja von der Macht eingesetzt, die Macht verläuft über sie und durch sie hindurch.“²⁹

Macht ist also nicht Eigentum einer Person, eines Subjekts, vielmehr ist sie ein omnipräsentes Phänomen – eine strategische Position. Sie spannt sich wie ein Netz zwischen Menschen sowie gesellschaftlichen Anforderungen und Einrichtungen. Man muss sich die Macht wie eine immerwährende Schlacht vorstellen – als ein komplexes und heterogenes Geflecht von Machtbeziehungen, die Änderungsprozessen unterworfen

27 Ruoff, Michael (2009): S. 217 - 218

28 Seier, Andrea (2001): S. 91

29 Foucault, Michel (1994): S. 38

sind (Unruheherde, Kämpfe, (vorübergehende) Umkehrung der Machtverhältnisse).³⁰

Durch diese 'Mikrophysik der Macht' würde in der Historie ein feldartiges Ganzes entstehen, welches die Produktivität der Macht belege und eine an Personen gebundene Macht gleichzeitig ausschliesse, so Foucaults Argumentation.³¹

3.2 Die Disziplinarmacht

Die Disziplinarmacht löst im 18. Jahrhundert die feudal-absolutistische Macht ab. „War der feudale Machttyp vertikal und absolut hierarchisch organisiert, so zeigt die Macht der milden Mittel die völlig neue Eigenschaft der horizontalen[, dezentralen] Organisation.“³² Die dahinterstehenden Disziplinartechniken greifen lückenlos ineinander und durchdringen den gesamten Gesellschaftskörper.

„Diese Methoden, welche die peinliche Kontrolle der Körpertätigkeiten und die dauerhafte Unterwerfung ihrer Kräfte ermöglichen und sie gelehrig/nützlich machen, kann man die »Disziplinen« nennen.“³³

Ihr Ziel ist die Dressur der Körper und das damit verbundene ökonomische Nutzbar-Machen. Es handelt sich bei der Disziplin um eine individualisierte Machttechnik bei der es um Überwachung, Verhaltens- und Eignungskontrolle, Leistungssteigerung und Verbesserung der Fähigkeiten eines Individuums geht. Verhalten, das von der gesetzten Norm, dem Normalverhalten, abweicht, wird von einer Mikro-Justiz korrigiert (normierende Sanktion).³⁴

Die zwei zentralen Disziplinartechniken sind die hierarchische Überwachung und die normierende Sanktion. Eine Kombination der Beiden spiegelt sich in der Prüfung wieder. Es entsteht ein Mikroskop des Verhaltens, welches das Individuum an den Beobachtungs-, Dressur- und Registrierapparat bindet. Am Ende folgt eine Selbstüberwachung.³⁵

30 Seier, Andrea (2001): S. 97

31 Ruoff, Michael (2009): S. 157

32 Ruoff, Michael (2009): S. 149

33 Foucault, Michel (1994): S. 175

34 Ruoff, Michael (2009): S. 102

Bogdal, Klaus-Michael (2008): S. 74

35 Seier, Andrea (2001): S. 98

Foucault spricht von der Disziplinarmacht, „wenn die Überwachung und Normierung der Tätigkeiten zu dauerhaftem, persönlichkeitsprägendem Verhalten führt.“³⁶

3.3 Der Panoptismus

3.3.1 Die Architektur

Jeremy Bentham entwarf 1787 ein Gefängnis, das aufgrund seiner architektonischen Beschaffenheit eine unablässige Kontrolle der Insassen gewährleistete. Dieses Gefängnis, welches er das Panoptikum nannte, besteht aus einem ringförmigen Gebäude in dem Zellen eingelassen sind, welche durch die ganze Tiefe des Gebäudes reichen und zum Mittelpunkt hin einsehbar, aber untereinander abgeschirmt sind. Ein Fenster in der Außenwand sichert die Ausleuchtung und somit die perfekte Einsehbarkeit der Zellen. Genau in der Mitte der Anlage befindet sich ein Turm in dem der Wächter postiert wird. Dieser Turm ist so beschaffen (Jalousien, Trennwände), dass er für die Häftlinge nicht einsehbar ist, gleichzeitig aber die Überwachung der Zellen perfekt gewährleistet. Der Gefangene wird zum „Objekt einer Information, niemals Subjekt in einer Kommunikation.“³⁷

Das Panoptikum wurde nicht nur als Gefängnis konzipiert, eine Übertragung auf den pädagogischen, medizinischen, militärischen oder ökonomischen Bereich ist ebenso denkbar.³⁸ Benthams Idee wurde zwar nie vollständig realisiert, dennoch setzten etliche Strafanstalten Teile davon um.³⁹

3.3.2 Die Wirkungsweise

Der Gefangene ist kontinuierlich der Überwachung des Aufsehers ausgeliefert, ohne ihn zu sehen. „Die Wirkung der Überwachung [...] ist permanent, auch wenn ihre Durchführung sporadisch ist.“⁴⁰ Der Insasse muss also von einer stetigen Überwachung ausgehen, obgleich diese nicht gewährleistet sein muss, ja sogar überflüssig sein kann. Die Macht muss dabei sichtbar, aber uneinsehbar sein – „der Häftling [darf] niemals

36 Bogdal, Klaus-Michael (2008): S. 74

37 Foucault, Michel (1994): S. 256 ff.

Zitat: Foucault, Michel (1994): S. 257

38 Wolf, Burkhardt (2008): S.280

39 Wolf, Burkhardt (2008): S.280

40 Foucault, Michel (1994): S. 258

wissen [...], ob er gerade überwacht wird, aber er muss [sich] sicher sein, daß er jederzeit überwacht werden kann.“⁴¹ Durch den Überwachungsdruck entsteht eine präventive Wirkung.

Foucault versteht das Panoptikum als „eine Maschine, die ein Machtverhältnis schaffen und aufrechterhalten kann.“⁴² Dieses Machtverhältnis automatisiert und entindividualisiert die Macht. Die Aufgabe des Aufsehers kann dabei nahezu jede Person wahrnehmen – er ist problemlos austauschbar. Es ist kein Souverän mehr vonnöten, da die Maschine die Machtasymmetrie, das Machtgefälle sicherstellt. Es entsteht eine fiktive Beziehung, die die Unterwerfung möglich macht. Dadurch können die unterschiedlichsten Personen zu den verschiedensten Dingen gezwungen werden (Verurteilter zu gutem Verhalten; Schüler zum Eifer, Arbeiter zur Arbeit), ohne das Zwang oder Gewalt eingesetzt werden muss. Die Zwangsmittel der Macht werden vielmehr von dem Internierten übernommen – er „spielt sie gegen sich selber aus [...] [und] wird zum Prinzip seiner eigenen Unterwerfung.“⁴³

3.3.3 Das panoptische Prinzip

Die Leitidee hinter dem panoptischen Prinzip bildet Benthams Panoptikum und dessen Wirkungsweise. Durch die Bündelung und Verallgemeinerung der Disziplinen im Panoptikum stellt dieses eine politische Technologie dar und ist von seiner spezifischen Verwendung ablösbar. Es programmiert auf der Ebene eines einfachen und leicht zu übertragenden Mechanismus, das elementare Funktionieren einer von Disziplinarmechanismen vollständig durchsetzten Gesellschaft.“⁴⁴ Es könne Anwendung finden, wann immer man es mit einer Vielzahl von Individuen zu tun hat, denen ein Verhalten oder eine Aufgabe aufgezwungen werden soll, so Foucault.⁴⁵ Häufig wird dieses Prinzip in der Wissenschaft auf Überwachungskomplexe wie etwa CCTV (Videoüberwachung) angewandt.

41 Foucault, Michel (1994): S. 259

42 Foucault, Michel (1994): S. 258

43 Foucault, Michel (1994): S. 260

44 Foucault, Michel (1994): S. 268

45 Foucault, Michel (1994): S. 263 ff.

Ruoff, Michael (2009): S. 159 ff.

4. Analyse

Im folgenden möchte ich nun die Vorratsdatenspeicherung im Hinblick auf ihre panoptischen Züge analysieren. Daher habe ich die wichtigsten Elemente des panoptischen Prinzips abgeleitet und geordnet. Ich werde diese nun Schritt für Schritt auf die Vorratsdatenspeicherung anwenden und dabei diskutieren inwieweit diese zutreffen.

4.1 Anwendbarkeit des panoptischen Prinzips

Angewendet werden kann das panoptische Prinzip nach Foucault immer wenn es sich um eine Vielzahl von Individuen handelt, denen ein Verhalten oder eine Aufgabe aufgezwungen werden soll.⁴⁶

4.1.1 Vielzahl von Individuen

Bei der Vorratsdatenspeicherung handelt es sich um eine EU-Richtlinie bzw. deren Umsetzung in ein deutsches Gesetz. Es sind also alle Menschen die moderne Kommunikationsmittel nutzen und in der EU leben betroffen – ausgenommen, die Länder in denen die Vorratsdatenspeicherung (noch) nicht umgesetzt oder (vorübergehend) ausgesetzt wurde. Den modernen Kommunikationsmitteln kann sich bereits heute kaum noch jemand entziehen. Die Benutzung von Internet und Handys sind nicht nur alltägliche, sondern auch essentielle Methoden des sozialen Umgangs, daher „ist die Einschätzung, dass alle Bürger betroffen sein werden, nicht zu hoch gegriffen.“⁴⁷ Die Zahl der Festnetzanschlüsse beläuft sich in Deutschland 2007 auf 38,12 Millionen, demgegenüber stehen 97,2 Millionen Mobilfunkteilnehmer.⁴⁸

4.1.2 Aufzwingen eines Verhaltens oder einer Aufgabe

Das Recht, insbesondere das Strafrecht dient der Sozialkontrolle. Es soll die „Befolgung von gesellschaftlichen Normen und damit Konformität erreicht“⁴⁹ werden. Das Verhalten und die Wertungen von Menschen werden durch das Recht beeinflusst. Die

46 Foucault, Michel (1994): S. 263 ff.

47 Engling, Dirk (2008): S. 71 – 72

48 Schaar, Peter (2008): S. 9

49 Grafe, Adina (2008): S. 4

Vorratsdatenspeicherung stellt ein Mittel zur Umsetzung des Rechts dar, es ermöglicht die Feststellung nicht normkonformen Verhaltens sowie die Identifizierung von Straftätern.⁵⁰

Die Verwendung der Vorratsdatenspeicherung war bei ihrer Einführung 2008 sehr weit gehalten worden. Verbrechen, die mittels Telekommunikation begangen werden wurden explizit berücksichtigt. Im speziellen die modernen Kommunikationsmittel sollen also dem Recht unterworfen werden und das bisher als teilweise rechtsfreier Raum geltende Internet verrechtlicht werden.⁵¹

Es soll also ein mit dem Gesetz konformes Verhalten, im speziellen im Internet, durch weitreichendere Ermittlungswerkzeuge und den dadurch entstehenden Druck erzwungen werden.

4.2 Asymmetrie durch die Maschinerie des Panoptikums

Das panoptische Prinzip legt das Bild einer Maschine zu Grunde, die ein Machtverhältnis schaffen und aufrechterhalten kann. Sie produziert eine Asymmetrie im Machtverhältnis, ein Souverän wird dadurch unnötig. Die Überwacher sind austauschbar.⁵²

Die Vorratsdatenspeicherung kennt mehrere Instanzen, die die Überwachung ermöglichen. Neben der Staatsanwaltschaft, die den Auftrag zum Abruf der Daten gibt und die Ermittlungen leitet, sind hier die Provider, die die Daten erheben und speichern und die Polizei, die auf die Daten zugreift und diese auswertet, zu nennen. Der Datenaustausch findet vollautomatisiert statt. Einige Rädchen der Vorratsdatenspeicherung sind also auch real Maschinen.

Als deutsche Besonderheit wird in die vollautomatisierte Weitergabe der Daten ein Richtervorbehalt integriert. Wie bereits beschrieben, stellt die IP-Abfrage eine Ausnahme dar. Der Richter soll dabei die Einhaltung der Norm gewährleisten, so dass sich auch die Vorratsdatenspeicherung innerhalb der Normen bewegt. Diese Kontrolle findet aber in der Realität nur bedingt statt. Eine Aktenauswertung des Max-Planck-

50 Grafe, Adina (2008): S. 4

51 Bundesverfassungsgericht (2010)

Ziercke, Jörg (2007): S. 2, 9

52 Ruoff, Michael (2009): S. 161

Institutes ergab, dass nur ganz selten Anordnungen zum Datenabruf abgelehnt bzw. Änderungen (in 1,7% der ausgewerteten Fälle) am Antrag durchgeführt werden. Eine darüberhinaus durchgeführte Expertenbefragung erhärtete den Eindruck, dass der Richtervorbehalt seine Kontrollfunktion nur bedingt erfüllt.⁵³

Die Macht entfaltet ihre Wirkung durch die Maschine. In ihr nehmen unterschiedliche, relativ leicht austauschbare Personen Funktionen wahr. Die einzelnen Instanzen kontrollieren sich gegenseitig. Beispielsweise prüft ein Richter die Einhaltung der Normen, das Telekommunikationsunternehmen prüft den Gerichtsbescheid.

Die Instanzen entscheiden über die Auswertung und erstellen die Ergebnisse der Vorratsdatenspeicherung – ein Souverän ist nicht nötig, da eine asymmetrische Machtverteilung stattfindet.

Es entsteht eine Machtbeziehung zwischen dem Überwachten und dem Überwachenden ohne dass diese sich 'kennen' müssen. Die Machtbeziehung ist asymmetrisch, da der Überwachte keinerlei Einfluss auf die Überwachung nehmen kann. Er erfährt, wenn überhaupt, nur die Folgen der Überwachung.

4.3 Trennung von sehen und gesehen werden

Eine sehr wichtige Rolle spielt beim Panoptikum die Sichtbarkeit. Das Gefängnis ist so angelegt, dass es eine perfekte Einsehbarkeit der Zellen gewährleistet – mit nur einem Blick ist es möglich viele Insassen zu sehen und ihr Verhalten auf Konformität zu prüfen. Dabei darf der Überwachte keinen Hinweis darauf bekommen, ob er gerade überwacht wird oder nicht.

4.3.1 Uneinsehbarkeit der Überwachung

Bei der Vorratsdatenspeicherung handelt es sich um eine verdeckte Maßnahme, deren Kennzeichen die Geheimhaltung der Maßnahme vor dem Betroffenen, sowie teilweise den Miteinbezug einer Vielzahl nicht verdächtiger Personen ist⁵⁴. Dabei werden auch etwaige Zeugnisverweigerungsrechte außer acht gelassen und es können vertrauliche

⁵³ Albrecht, Hans-Jörg / Grafe, Adina / Kilchling, Michael (2008): S. 410

⁵⁴ Beispielsweise können alle in einer Funkzelle eingebuchten Mobiltelefone abgefragt werden, so auch die Nummern vieler Unbeteiligter, weil sie sich zur Zeit eines Verbrechens in der Nähe dessen Ortes befanden.

und intime Daten erfasst werden. Im Zuge dessen werden Informationen generiert, die nicht nur die Vergangenheit, sondern auch die Zukunft bzw. das Vorfeld einer vermeintlichen Straftat betreffen.⁵⁵

Die Speicherung der Daten findet bei verschiedenen privaten Unternehmen statt. Ob auf sie zugegriffen wird, wird dem Betroffenen, wenn überhaupt, nur im Nachhinein mitgeteilt. Das Max Planck Institut zog Akten-Stichproben vergangener Verkehrsdatenabfragen und wertete diese aus. Laut dieser Studie konnten ein Drittel der Beschuldigten über die Akteneinsicht Wissen über die Nutzung der Verkehrsdaten erlangen. Nur 4% wurden per Aktenbeschluss informiert. Eine Vernichtung der Daten konnte den Akten nur in 3% der Verfahren entnommen werden.⁵⁶ Eine rechtliche Aufklärungspflicht besteht nicht.

Das Bundesverfassungsgericht verlangt allerdings in seinem Urteil von einer zukünftigen Vorratsdatenspeicherung eine Benachrichtigungspflicht. Diese setzt aber dennoch erst nach der Überwachung ein.⁵⁷

Die Verkehrsdaten dürfen nicht eingesehen werden. Ein Antrag eines Politikers auf Einsicht wurde mit dem Verweis auf die Datenschutzrechte der Telekommunikationspartner von der Bundesnetzagentur abgelehnt.⁵⁸

Welche Verdachtsmomente und Analysen aus den Vorratsdaten gezogen werden bleibt, ob der Unkenntnis der Daten sowie der verwendeten Analysemethoden, für den Überwachten ebenfalls nicht nachvollziehbar. Das Bundesverfassungsgericht verlangt aber in seinem Urteil, dass zukünftig Verfahrensregeln über die Auswertung der Daten zu erlassen sind.⁵⁹ Dadurch würde möglicherweise etwas klarer, was mit den Daten geschieht.

Es können mittels sogenannten 'Stillen SMS' sogar Verkehrsdaten ohne das Wissen des Überwachten erzeugt werden. Dem Überwachten können beispielsweise vom BKA 'Stille SMS' im Fünfminutentakt gesendet werden. Diese sind im Prinzip ganz normale SMS die aufgrund einer Information in der SMS aber vom empfangenden Gerät nicht

55 Albrecht, Hans-Jörg / Grafe, Adina / Kilchling, Michael (2008): S. 3 - 4

56 Albrecht, Hans-Jörg / Grafe, Adina / Kilchling, Michael (2008): S. 103 – 104, 411

57 Bundesverfassungsgericht (2010)

58 Schaar, Peter (2009): S. 16

Spitz, Malte

59 Schneider, Adrian (2010)

angezeigt werden. Dadurch werden ohne das Wissen des Überwachten dauernd Verkehrs- und Standortdaten erzeugt, die wiederum über eine Verkehrsdatenabfrage abgerufen werden können.⁶⁰

Der Überwachte kann also grundsätzlich nur im Nachhinein nachvollziehen ob er überwacht wurde. Eine Einsicht in die Funktionsweise des Systems kann er nicht erlangen.

4.3.2 Sichtbarkeit der Überwachten

Die Inhaltsanalyse von Kommunikation ist sehr aufwendig, teuer und fehleranfällig. Die Analyse der Verkehrsdaten hingegen kann vollautomatisiert stattfinden und ist häufig deutlich aufschlussreicher als die Inhaltsanalyse.⁶¹

Im folgenden werde ich nun die Möglichkeiten und Einschränkungen bei der Auswertung der Vorratsdaten sowie die Umgehungsmöglichkeiten genauer beleuchten. Dies ist notwendig um die Frage nach der Sichtbarkeit des Individuums beantworten zu können.

a) Extraktion von Wissen aus Verkehrsdaten

Beziehungen zu anderen Personen und Verhalten

In den Verkehrsdaten nur einer Person spiegeln sich nahezu alle sozialen Kontakte wieder. Es können aber auch Beziehungsintensitäten abgeleitet werden: „Mit wem kommuniziert die Person wann, wie oft, über welche Kommunikationsart, wie lange und in welchem zeitlichen Kontext zu bestimmten Ereignissen?“⁶²

Aus langer und häufiger Kommunikation lässt sich eine engere soziale Bindung ableiten. Es kann zwischen geschäftlichen Kontakten, die innerhalb üblicher Geschäftszeiten stattfinden, und privaten differenziert werden. Beziehungspartner können anhand der Intensität der Kommunikation, welche auch während üblicher Geschäftszeiten und Auslandsaufenthalten anhält, identifiziert werden. Ebenso kann eine Affäre aus den Daten herausgelesen werden. Auch spielen die Orte der eingebuchten Handys eine zentrale Rolle bei der Analyse der Beziehungen.

60 Schaar, Peter (2009): S. 6 - 7

61 Engling, Dirk (2008): S. 72 - 73

62 Kurz, Constanze / Rieger, Frank (2009): S. 8

Durch die Verknüpfung mit weiteren Daten entsteht ein noch klareres Bild. Wurde zum Beispiel einige Zeit zuvor ein Hotel gebucht an dessen Ort sich die beiden Telefone treffen? Die Daten können aber auch mit externen Quellen abgeglichen werden z.B. mit dem Bankkonto, Buchungsinformationen von Verkehrsmitteln (Mietwagen, Bahn etc.) oder Hotels.⁶³

Rückschlüsse auf persönliche Lebenssituation

Rückschlüsse auf die momentanen Lebensumstände von Personen sind vielfältig:

„So ließe sich beispielsweise aus einem E-Mail-Kontakt mit einem auf Familienrecht spezialisierten Anwalt gefolgt von telefonischen Anfragen bei Wohnungsmaklern eine Scheidungsabsicht prognostizieren. Kontakte zu Konflikt- und Schwangerschaftsberatungen, spezialisierten Ärzten, Prostituierten, Telefonsex-Hotlines, spezialisierten Versandhändlern, Kreditvermittlern, Jobcentern, Umzugsservices, Interessenverbänden etc. ergäben aus einer minimalen Datenmenge jeweils umfangreiche Rückschlüsse auf das Privatleben eines Betroffenen.“⁶⁴

Netzwerkanalyse

Die Analyse der Vorratsdaten beginnt mit einem Datenabruf der Kommunikationsdaten einer bestimmten Person. Daraufhin werden die Daten der (wichtigsten) Kontaktpersonen abgerufen und auf Verbindungen untereinander untersucht. Menschen die innerhalb eines Sozialgefüges eine zentrale Rolle spielen lassen sich identifizieren. Es lässt sich des Weiteren feststellen ob es sich um eine lose Gruppe, um eine familiäre oder eine hierarchische Struktur handelt. Es können ähnliche Kommunikationsketten erkannt werden, die von bestimmten Kontakten ausgelöst werden. Es können dabei Annahmen getroffen werden welches Ereignis diese hervorrief. So kann beispielsweise eine Person als sehr bedeutend für eine Umweltschutzgruppe erkannt werden – ohne das dies dieser bewusst sein muss. „Durch Beeinträchtigung der Handlungsfähigkeit einer einzelnen Person kann dann mit minimalem Aufwand die Wirksamkeit einer ganzen Gruppe oder Bewegung behindert werden.“^{65 66}

63 Kurz, Constanze / Rieger, Frank (2009): S. 7 – 10, 12

64 Kurz, Constanze / Rieger, Frank (2009): S. 10

65 Kurz, Constanze / Rieger, Frank (2009): S. 7 – 11

Zitat: S. 11

66 In den Niederlanden gibt es ein 'Projekt Gegenwirken', welches Personen die Geheimdiensten oder

b) Beschränkungen beim Abruf der Daten

Die oben genannten Schlüsse können logischerweise erst nach Abruf der Daten bei den verschiedenen Providern erfolgen. Dem Abruf der Daten sind aber verschiedene Schranken seitens des Gesetzgebers und des Bundesverfassungsgerichts gesetzt worden. Bei den meisten Abfragen gilt ein Richtervorbehalt, wie unter Punkt 4.2 beschrieben. Dort habe ich bereits dargelegt, dass dieser Schutz nicht sonderlich effektiv ist. Dennoch stellt er eine gewisse Hürde dar.⁶⁷

Mit der Einführung der Vorratsdatenspeicherung durften die Daten nahezu in jedem Fall abgerufen werden. Die Gefahrenabwehr, alle Straftaten sogar bis hin zu Ordnungswidrigkeiten rechtfertigten das Mittel. Das Bundesverfassungsgericht erlässt daraufhin im März 2008 eine einstweiligen Anordnung, welche die Maßnahme nur noch bei schweren Straftaten gestattet.⁶⁸ In ihrem darauffolgenden Urteil zur Vorratsdatenspeicherung im März 2010 verlangen die Richter eine Liste mit Straftaten für die die Daten verwendet werden dürfen und verlangt generelle Ausnahmen für Kommunikationsdaten die bei Beratung im sozialen oder kirchlichen Bereich entstehen.⁶⁹

Diese Strenge gilt allerdings nicht für die Zuordnung von Bestandsdaten zu IP-Adressen, da diese das Gericht für weniger schützenswert hält. Des Weiteren gilt sie nicht für die herkömmliche Abfrage der zu Abrechnungszwecken gespeicherten Verkehrsdaten, auf die ein Zugriff seit 2002 möglich ist.⁷⁰

Polizei suspekt erscheinen, denen jedoch keine konkreten Straftaten nachgewiesen werden können, mit vielen legitimen Einzelmaßnahmen konfrontiert. Beispielsweise mit einer umfangreicheren Steuerprüfung, häufige Kontrollen der Gewerbeaufsicht etc. Es scheint so, als habe die Person 'Pech' gehabt, allerdings werden die meisten der Maßnahmen zufällig von einem Computerprogramm ausgelöst. Ihr politisches, privates, berufliches und gesellschaftliches Engagement lässt sich über den erzeugten Leidensdruck erheblich stören.

67 Bundesverfassungsgericht (2010)

68 Schröder, Burkhard (2008)

69 Bundesverfassungsgericht (2010)

70 Bundesverfassungsgericht (2010)
Schröder, Burkhard (2008)

c) Umgehung der Vorratsdatenspeicherung

Anonymer Internetzugriff

Über sogenannte Anonymisierungsdienste kann die IP-Adresse verschleiert werden. Diese Dienste schalten einen oder mehrere Server zwischen Client und angefragten Server. Der angefragte Server bekommt nur die IP-Adresse des zwischengeschalteten Rechners. Die Verbindung zwischen den Rechnern findet meist verschlüsselt statt. Die zwischengeschalteten Computer dürfen kein Logging (das mitprotokollieren der Verkehrsdaten) betreiben.⁷¹ Eine Rückverfolgung mittels der IP-Adresse endet so immer bei einem der zwischengeschalteten Server. Die Vorratsdatenspeicherung sah auch eine Protokollierung bei diesen Anonymisierungsdiensten vor und führte diese so ad absurdum. Allerdings waren von dieser Regelung nur Rechner in Deutschland betroffen.⁷²

Bei mobilem Internet mittels UMTS werden die IP-Adressen momentan für mehrere Anschlüsse verwendet, eine Zuordnung ist nicht möglich. Das surfen ist faktisch anonym.⁷³

Anonyme Kommunikation

Die Vorratsdatenspeicherung kann beim Telefonieren über die Benutzung von öffentlichen Telefonzellen, durch die Benutzung von anonymen Prepaid oder ausländischen Mobiltelefonen umgangen werden. Letztere müssen logischerweise aus Ländern stammen die keine Vorratsdatenspeicherung praktizieren – diese können auch in Deutschland problemlos genutzt werden. Wechselt man die Geräte und Karten häufig kann ein relativ hoher Anonymisierungsgrad erreicht werden.⁷⁴

Die Kommunikation per E-Mail kann über sogenannte Remailer komplett anonymisiert werden, diese funktionieren ähnlich wie die oben beschriebenen Anonymisierungsdienste. Weitere Möglichkeiten sind die Nutzung ausländischer E-Mailanbieter oder Wegwerf-E-Mail-Adressen, welche nur kurze Zeit genutzt werden können. Alternativ dazu kann auch auf Webforen oder Nachrichtendienste innerhalb von

71 Kubieziel, Jens (2007): S. 47 - 52

72 AK Vorratsdatenspeicherung

73 Vetter, Udo (2010)

74 Engling, Dirk (2008): S. 75 - 77

Webseiten zurückgegriffen werden.⁷⁵ Es können natürlich auch offene W-LAN-Spots oder Internetcafés benutzt werden, hierbei kann aber zumindest eine Lokalisierung bis zum Ausgangspunkt und somit eine Zeit-Ort-Bestimmung stattfinden.

Problem: Redundanz der Daten

Die Daten werden redundant gespeichert, sie fallen immer bei beiden Kommunikationsteilnehmern an.⁷⁶ Daher müssen auch beide Anonymisierungsstrategien verfolgen, da ansonsten zumindest ein Teil, wenn nicht alle, Daten rekonstruiert werden können.

Für die organisierte Kriminalität oder Terroristen sollte es ein Leichtes sein diese Kommunikationsmittel in ihren Netzwerken zu nutzen. Für den Privatmensch gestaltet sich die Nutzung aber schwierig, da zum einen das Wissen über die Möglichkeiten fehlt, zum anderen auch die Kommunikationsteilnehmer mitziehen müssten.

Eine staatliche Interventionsmöglichkeit bietet das Verbot derartiger Dienste oder den Zwang zur Mitprotokollierung der Vorratsdaten. Da das Internet aber nur bedingt Grenzen kennt ist eine Umgehung mit dem entsprechenden Know How praktisch immer möglich.⁷⁷

d) Sichtbarkeit und Überprüfung der Konformität

Die Beispiele zeigen deutlich, dass eine Sichtbarkeit bis in die privatesten Räume möglich ist, gleichzeitig die Vorratsdatenspeicherung aber auch mit relativ einfachen Mitteln umgangen werden kann. So ist weniger die organisierte Kriminalität oder der Terrorismus von der Überwachung betroffen, da diese sich normalerweise im Klandestinen bewegen. Das Entdeckungsrisiko wird dabei einkalkuliert und möglichst weit abgesenkt.⁷⁸

Vielmehr kann Kontrolle nur über die ausgeübt werden, die sich entweder nicht zu schützen Wissen und / oder in (Beziehungs-)Netzwerke eingebettet sind, die eine geschützte Kommunikation nicht beherrschen.

⁷⁵ Engling, Dirk (2008): S. 77

Kubieziel, Jens (2007): S. 27 - 46

⁷⁶ Engling, Dirk (2008): S. 72

⁷⁷ Engling, Dirk (2008): S. 75

⁷⁸ Albrecht, Hans-Jörg / Grafe, Adina / Kilchling, Michael (2008): S. 7

Deren Verhalten ist minutiös nachvollziehbar und darüber auch auf Konformität prüfbar. Die einzig verbliebenen (Zugriffs-)Schranken sind die des Bundesverfassungsgerichts bzw. des Gesetzes.

Dabei wird die Datenmenge in Zukunft tendenziell zunehmen. Mobile Dienste und Geräte erobern immer weitere Bereiche. Als Beispiele seien hier Bezahldienste per Handy, Mautsysteme oder Gesundheitsmonitoring zu nennen – dabei muss den Betroffenen nicht unbedingt klar sein, dass sie gerade Verkehrsdaten erzeugen.⁷⁹

4.4 Die bewusste Überwachung

Auf die Trennung der Sichtbarkeit des Überwachten und der Unsichtbarkeit des Überwachenden baut die Sichtbarkeit des Überwachungssystems auf. Der Überwachte muss sich stets überwacht fühlen, sich bewusst sein, dass er jeden Moment überwacht werden kann. Daraus ergibt sich eine kontinuierliche Wirkung der Überwachung, obwohl ihre Durchführung nur sporadisch ist oder gar unterbleiben kann.

Die Sichtbarkeit der Überwachung findet vor allem über die Aufklärung der Medien statt, da die Vorratsdatenspeicherung selbst komplett verdeckt abläuft. Die Berichterstattung wurde dabei vor allem durch den Streit der Befürworter und Gegner hervorgerufen.

Die Berichterstattung in Deutschland ist hauptsächlich ereignisbasiert. Die Medien verlieren sehr schnell das Interesse an einem Thema, wenn sich keine Nachrichten mit Neuigkeitswert ergeben. Die „Medienunternehmen [sind] in demokratischen und marktwirtschaftlich organisierten Gesellschaften davon abhängig [...], dass ihre Angebote vom Zuschauer angenommen und genutzt werden“.⁸⁰ Ansonsten bleiben Werbeeinnahmen und / oder Verkaufseinnahmen bzw. die Legitimation der öffentlichen Finanzierung bei öffentlich-rechtlichen Medien aus.⁸¹

Es ist davon auszugehen, dass die Berichterstattung abebbt sobald der Streit beigelegt ist. Nur bei bedeutungsvollen Ereignissen in Bezug auf die Vorratsdatenspeicherung (möglicherweise auftretenden Datenskandalen, Ermittlungserfolgen, der Einführung oder Verwendung weiteren andersartigen Überwachungsmaßnahmen etc.) ist wieder mit

79 Kurz, Constanze / Rieger, Frank (2009): S. 30 - 33

80 Hickethier, Knut (2003): S. 174

81 Hickethier, Knut (2003): S. 174

einer Berichterstattung zu rechnen.⁸²

Der Streit zwischen den Befürwortern und Gegnern der Vorratsdatenspeicherung hat dieser einen immensen Bekanntheitsgrad unter den Menschen beschert. Dies kann zum einen mit dem medialen Hype, der beispielsweise auch um die knapp 35'000 Verfassungsbeschwerden und deren Verhandlung entstanden ist, zum Anderen aber auch mit Umfragen belegt werden.⁸³ Nach einer repräsentativen Forsa-Umfrage im Auftrag des Arbeitskreis Vorratsdatenspeicherung vom Mai 2008 wissen 73% der Bundesbürger von der Speicherung der Verbindungsdaten.⁸⁴

Dieser hohe Bekanntheitsgrad verknüpft mit der vermuteten, deutlich geringeren Berichterstattung in der Zukunft, ergibt zumindest eine teilweise Erfüllung der stetigen Sichtbarkeit. Sicher ist diese nicht mit der Stetigkeit des panoptischen Turmes zu vergleichen, dennoch ist davon auszugehen, dass die Vorratsdatenspeicherung in den Köpfen ist und durch eine gelegentliche Auffrischung durch oben genannte Ereignisse auch bleibt.

Verknüpft mit den weiteren Überwachungsmaßnahmen ist es denkbar, dass ein Eindruck des stetigen überwachtseins aus der Vielzahl der Instrumente entsteht und auch das Internet nicht (mehr) als rechtsfreier Raum, sondern vielmehr als besonders überwachter Raum, wahrgenommen wird.

Eine Besonderheit ist dabei, dass die Medienaufmerksamkeit und -berichterstattung hauptsächlich durch den Streit um die Vorratsdatenspeicherung und damit von den Gegnern selbiger hervorgerufen wurde.⁸⁵

Aber auch die Polizei informierte über die Vorratsdatenspeicherung. Aufgrund der ablehnenden Haltung der deutschen Bürger⁸⁶ und vor allem des deutschen Bundestages,⁸⁷ allerdings mit einer Strategie, die vor allem auf die Notwendigkeit der Vorratsdatenspeicherung zur Bekämpfung schwerer Verbrechen abzielt.⁸⁸ Nichts desto trotz wiesen auch sie häufig auf die, dabei zwar positiv besetzte, Wirkung hin.

Die Wirkung bleibt letzten Endes die Selbe, ein Großteil der Menschen weiß von der

82 Hickethier, Knut (2003): S. 174

83 Heise Online (2010c)

84 Forsa (2008)

85 Deutscher Bundestag (2008): S. 6 - 7

86 Stern (2007)

87 Engling, Dirk (2008): S. 69

88 Ziercke, Jörg (2007): S. 2, 9

Vorratsdatenspeicherung. Dennoch muss konstatiert werden, dass diese Sichtbarmachung mit nichten der Sichtbarkeit des panoptischen Turmes gleicht, der wie ein Damoklesschwert über den Insassen schwebt. Die Sichtbarkeit ist also nur teilweise gegeben, da nicht jeder Überwachte ob seiner Überwachung weiß und die Kontinuität der Information über diese fehlt.

Die Überwachten helfen auch bei der Vorratsdatenspeicherung dem Überwacher. Die Daten werden von den Überwachten selbst generiert, ein ausweichen auf alternative Kommunikationsmöglichkeiten findet, wie oben beschrieben, nur bedingt statt.⁸⁹

4.5 Kontinuität der Überwachungswirkung

Das panoptische Gefängnis bietet die Möglichkeit der permanenten Überwachung bei relativ geringem Aufwand. Der Überwachte muss also davon ausgehen andauernd überwacht zu werden. Dies führt zu einer Verhaltensanpassung; Das überwachte Individuum kontrolliert sich selbst. Die Überwachungswirkung wird allein durch die Möglichkeit der Überwachung erzielt und macht sie dadurch entbehrlich.

4.5.1 Permanente Überwachung

Die Provider sind gesetzlich verpflichtet die Daten über den Zeitraum von sechs Monaten zu speichern und in Reaktion auf eine legitime Anfrage an die entsprechende Stelle auszuhändigen. Eine Auswertung der Daten ist also über das komplette vergangene halbe Jahr möglich, kann aber ebenso in die Zukunft⁹⁰ gerichtet sein. Sie findet also nicht nur in diesem Moment statt, sondern ist auch vergangenheitsbezogen und in die Zukunft gerichtet.⁹¹

Der Überwachte muss folglich davon ausgehen permanent überwacht zu werden bzw. überwacht werden zu können.

89 Lyon, David (2006): S. 609

90 Die Verwendung der Daten zur Gefahrenabwehr wurde vom Bundesverfassungsgericht mit seiner einstweiligen Anordnung außer Kraft gesetzt. Nach dem darauf folgenden Urteil muss die Verwendung gesetzlich spezifiziert werden.

91 Bundesgesetzblatt (2007): 3205 - 3209

4.5.2 Verhaltensanpassung und -änderung

Ob durch die Vorratsdatenspeicherung eine Verhaltensanpassung stattfindet ist umstritten. Laut einer repräsentativen Forsa-Umfrage haben 11% der Bundesbürger in den ersten 5 Monaten der Vorratsdatenspeicherung in Deutschland aufgrund dieser in bestimmten Fällen auf die Kommunikation mittels E-Mail, Telefon oder Handy verzichtet. Zu sensiblen Einrichtungen (Drogenberatung, Psychotherapeut etc.) würden 52% der Befragten seit der Speicherung der Verbindungsdaten keinen Kontakt mehr per Telefon, E-Mail oder Handy suchen. 6% haben den Eindruck das seit dem weniger Menschen Kontakt mit ihnen über diese Medien aufnehmen.⁹²

Es findet also eine Anpassung im Kommunikationsverhalten statt. Ob stattdessen auf andere Kommunikationsformen ausgewichen wurde oder schlichtweg gar nicht mehr kommuniziert wurde erfragte die Studie nicht. Ob eine Anpassung im realen Leben stattfand, beispielsweise das Unterlassen von Copyrightverletzungen im Internet oder anderer Straftaten lässt sich aus der Umfrage ebenfalls nicht ableiten. Leider gibt es keine weiteren Studien die sich explizit auf eine mögliche Verhaltensänderung durch die Vorratsdatenspeicherung beziehen. Hier besteht dringend empirischer Forschungsbedarf.

Ob ein sogenannter 'chiling effect' (Nichtgebrauch von Freiheitsrechten) durch die Vorratsdatenspeicherung herbeigeführt wird ist mangels Studien bisher empirisch nicht nachweisbar, dennoch ist es sehr wahrscheinlich.⁹³ Das Bundesverfassungsgericht stellt in seinem Urteil zur Vorratsdatenspeicherung fest, dass diese ein „besonders schwere[r] Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“⁹⁴ ist. Da die Verwendung der Daten unbemerkt stattfindet ist sie „geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.“⁹⁵

Eine Auswirkung auf die Kriminalitätsrate ist in Ländern wie Irland die schon länger Vorratsdaten speichern nicht nachweisbar. Eine Unwirksamkeit der Vorratsdatenspeicherung kann aber daraus noch nicht abgeleitet werden. Beispielsweise kann sie

92 Forsa (2008): S. 2 - 4

93 Maras, Marie-Helen (2009): S. 78 - 79

94 Bundesverfassungsgericht (2010)

95 Bundesverfassungsgericht (2010)

mittels Professionalisierung umgangen werden. Manche Straftaten treten aber auch möglicherweise erst durch die Einführung der Vorratsdatenspeicherung auf, da von Beratungsgesprächen im Vorfeld abgesehen wird.⁹⁶

Betroffen ist auch die Presse und darüber letztlich auch das demokratische Prinzip der vierten Gewalt. Ein Informantenschutz kann mit einer Vorratsdatenspeicherung kaum noch gewährleistet werden.⁹⁷

Findet eine Verhaltensänderung statt muss diese, bei einer derartig abstrakten Überwachung, internalisiert werden, d.h. der Überwachte beginnt sein Verhalten und letzten Endes sich selbst zu überwachen – als Reaktion auf die Überwachung und aus Angst vor etwaigen Negativfolgen.

4.5.3 Kontinuierliche Wirkung der Überwachung

Wenn man aus Punkt 4.5.2 schließt, dass eine Verhaltensänderung zumindest bei einem Teil der Bevölkerung stattfindet, ist davon auszugehen, dass diese Wirkung auch erhalten bleibt wenn die Überwachung ohne Wissen des Überwachten aussetzt oder abgestellt wird.

Da der Betroffene sein Verhalten nur auf der Annahme des überwacht werdens ändert, ohne je genau zu wissen ob dies wirklich stattfindet, folgt in logischer Konsequenz daraus eine Unabhängigkeit der Verhaltensänderung von einer wirklichen Überwachung.

⁹⁶ Golem.de (2007)

⁹⁷ Wikileaks bietet allerdings die Möglichkeit Informanten Informationen anonym zu veröffentlichen. Auch ist denkbar, dass Journalisten Umgehungssysteme nutzen, was aber den Aufwand deutlich erhöht. Ob die Abschreckende Wirkung dadurch aufzuheben ist bleibt zu klären.

5. Fazit

5.1 Zusammenfassung der Untersuchung

Zu Beginn der Analyse der Vorratsdatenspeicherung mithilfe des panoptische Prinzips, welches Foucault aus Benthams Gefängnis Panoptikum ableitet, stellt sich immer die Frage der Anwendbarkeit. Diese ist gegeben, da die Vorratsdatenspeicherung, wie von Foucault gefordert, eine Vielzahl von Individuen, letzten Endes fast alle Bürger der Bundesrepublik betrifft und diese normiert. Die Normierung findet über das Gesetz statt, welches den Individuen seine Verhaltensregeln aufzwingt.

Durch die Vorratsdatenspeicherung entsteht eine Machtasymmetrie. Verschiedene, ersetzbare Personen entscheiden über die Überwachung und deren Auswirkung auf das Individuum. Dieses hat keinerlei Einfluss auf die Überwachung und hat nur deren Folgen zu tragen.

Die Machtwirkungen des Panoptikums entstehen vor allem durch die Trennung von sehen und gesehen werden. Durch die Uneinsehbarkeit der Überwachung ist nie klar ob gerade eine Überwachung stattfindet oder nicht. Die Vorratsdatenspeicherung ist eine verdeckte Maßnahme und bedient sich dadurch der Unsichtbarkeit. Eine Einsicht in die Daten oder deren Auswertung ist nicht möglich. Es besteht keine Informationspflicht. Das Bundesverfassungsgericht verlangt allerdings mit seinem Urteil vom 2. März 2010 eine solche. Diese setzt aber ebenfalls erst nach der Verwendung der Daten ein. Es kann mittels der sogenannten 'Stillen SMS' sogar eine unbemerkte Datenerzeugung stattfinden. Die Überwachung ist also für den Betroffenen nicht einsehbar. Umso besser kann allerdings der Überwachte gesehen werden. Die Daten der Vorratsdatenspeicherung lassen, bei normalem Telekommunikationsverhalten, umfassende Rückschlüsse auf die Lebensumstände des Betroffenen zu. Es können vollautomatisiert Beziehungen zu anderen Personen und das funktionieren von Netzwerken erkannt werden. Die Vorratsdaten nehmen durch die Entwicklung mobiler (Kommunikations-)Dienste immer weiter zu und lassen sich mit externen Daten verknüpfen, dadurch steigt die Aussagegenauigkeit immer weiter an.

Eingeschränkt wird die Sichtbarkeit des Überwachten durch die Beschränkung auf schwere Straftaten. Diese gilt erst seit der einstweiligen Anordnung des

Bundesverfassungsgerichts – zuvor war ein Zugriff auf die Daten auch in weniger schweren Fällen möglich (siehe Punkt 2.2.2). Ein Richtervorbehalt soll die Kontrolle sichern, in der Realität ist diese aber nicht stark ausgeprägt. Die größte Einschränkung der Sichtbarkeit des Überwachten sind die leichten Umgehungsmöglichkeiten der Vorratsdatenspeicherung. Diese können vor allem von Netzwerken genutzt werden. Für den Privatmensch sind sie nur schwer praktikabel.

Ebensowichtig für die panoptische Wirkung ist das Wissen um die Überwachung. Eine recht umfangreiche Aufklärung findet vor allem über die Medien statt, immerhin wissen 2008 73% der Menschen in Deutschland von der Vorratsdatenspeicherung. Aufgrund der ereignisbasierten Beschaffenheit der Medien wird deren Berichterstattung deutlich abnehmen (es wird nur bei neuen Ereignissen im Zusammenhang mit der VDS berichtet) wenn der Streit um die Vorratsdatenspeicherung beigelegt ist. Die stetige Sichtbarkeit der Überwachung wird also nur teilweise erfüllt. Es ist aber davon auszugehen, dass die Vorratsdatenspeicherung in den Köpfen der meisten Bürger ist. Dennoch werden dem Überwachungsmechanismus dadurch panoptische Züge genommen.

Als Folge aus der Trennung von sehen und gesehen werden, bei gleichzeitigem Wissen von der Überwachung, ergibt sich ein Überwachungsdruck der die Überwachten zu normkonformem Verhalten zwingt - selbst wenn sie nicht überwacht werden. Aufgrund der Analogie zum Panoptikum müsste sich auch bei der Vorratsdatenspeicherung eine Verhaltensanpassung ergeben. Eine Forsa-Umfrage ermittelte eine Absicht von 52% der Befragten sensible Stellen nicht mehr per E-Mail, Telefon oder Handy kontaktieren zu wollen. Ob eine Verhaltensanpassung in Richtung Normalverhalten stattfindet wurde bisher noch nicht erforscht. Es ist aber davon auszugehen das es eine panoptische Wirkung gibt. Wie stark diese ist, bleibt offen. Die Wichtigkeit von empirischen Studien in diesem Bereich kann nur ein weiteres Mal betont werden.

Aufgrund der Uneinsehbarkeit der Überwachung bleibt der Normierungseffekt auch beim Aussetzten der Überwachung bestehen – der Überwachte ändert sein Verhalten nur unter der Annahme das er überwacht wird. Diese Annahme wird von einem Aus- oder Wegfall der Überwachungsmaschinerie nicht tangiert.

5.2 Ergebnis der Analyse

Das panoptische Prinzip lässt sich sehr gut auf die Vorratsdatenspeicherung anwenden. Sie trennt genau wie das Panoptikum die verschiedenen Sichtbarkeitsbereiche voneinander ab, allerdings nicht mit der selben Perfektion. Das Leben des Überwachten kann zwar minutiös nachvollzogen werden, allerdings nur mit einer beschränkten Anwendungsbefugnis und der Möglichkeit des Überwachten sich der Überwachung zu entziehen (siehe Punkt 4.3.2). Durch diese Lücken können sich weniger die Normalbürger sondern gerade die Unangepassten entziehen. Hinzu kommt, dass das Wissen um die Überwachung, ohne das kein Überwachungsdruck erzeugt werden kann, nicht in voller Breite und Kontinuität gestreut wird.

Würden diese Probleme ausgemerzt, könnte nicht nur der Großteil der Gesellschaft überwacht und normiert werden, sondern auch das eigentliche oder angebliche Ziel der Vorratsdatenspeicherung, die Unangepassten zu normieren, erreicht werden.

Doch auch ohne die Lösung dieser Probleme führt eine erneute Umsetzung einen entscheidenden Schritt weiter in Richtung einer Normalisierungsgesellschaft, in der es keine oder kaum Verhaltensabweichungen von der Norm gibt. Wie stark der Beitrag der Vorratsdatenspeicherung zu dieser Entwicklung ausfällt hängt allerdings von der Umsetzung ab. Das Bundesverfassungsgericht hat mit seinen Einschränkungen den panoptischen Wirkungsgrad der Vorratsdatenspeicherung jedenfalls herabgesetzt.

5.3 Bewertung der Methode

Foucaults Panoptismus eignet sich sehr gut als Analysewerkzeug für die komplex-abstrakte Überwachungstechnik. Mit der Trennung des Paares 'sehen und gesehen werden' lässt sich die Vorratsdatenspeicherung sehr gut erklären. Eine panoptisch-präventive Wirkung lässt sich zwar empirisch mangels Studien nicht nachweisen, dennoch zeigt die Analyse mittels des panoptischen Prinzips, dass eine Machtwirkung vorhanden ist und diese verhaltensändernd wirkt. Eine Forsa-Umfrage gibt auch erste empirische Hinweise.

Die Erklärungen und Ergebnisse überzeugen. Die Vorratsdatenspeicherung lässt sich besser verstehen und enthält Funktionselemente die tatsächlich wie die panoptische Maschine, die Foucault beschreibt, funktionieren. Durch die ähnliche Struktur ergibt

sich während der Analyse auch eine ähnliche Wirkungsweise. Die Vorratsdatenspeicherung kann daher auch nie als reine Strafverfolgungstechnik gesehen werden, da immer auch die Machtwirkungen einer Überwachungstechnik mitschwingen.

Ein Problem mit dem sich Foucault nicht auseinandergesetzt hat sind Fehler der Überwacher. Was passiert, wenn der Überwacher normkonformes Verhalten als nicht normkonformes deutet oder die Überwachten verwechselt? Beim Panoptikum spielt das aufgrund dem direkteren Kontakt und der begrenzten Anzahl der Insassen nur bedingt eine Rolle. Bei komplex-abstrakten Überwachungstechniken wie der Vorratsdatenspeicherung hingegen können leicht Fehler unterlaufen. Z.B. kann ein Datensatz fehlerhaft sein oder IP-Adressen von Anderen mitverwendet werden. Den Daten wird aber absolutes Vertrauen geschenkt. Für den Überwachten ist nur schwer nachweisbar das er sich normkonform verhalten hat. Hinzu kommt, dass die Daten falsch interpretiert werden können und normkonforme Menschen plötzlich verdächtig werden. Dies kann zwar zu erhöhtem Überwachungsdruck führen, kann aber auch gegenteilige Wirkungen haben - beispielsweise bei einem Menschen der trotz nicht konformen Verhaltens nicht sanktioniert wird.

5.4 Schlussfolgerungen

Ein empirischer Nachweis der verhaltensändernden Wirkung steht dringend aus. Insgesamt kann die Vorratsdatenspeicherung als panoptisches System betrachtet werden, welches in seiner Implementierung einige Schwächen aufweist. Weiterer Forschungsbedarf besteht insbesondere auch über die Wechselwirkungen der unterschiedlichen Überwachungstechniken. Werden Schwächen und Probleme der einen Überwachungstechnik mit einer anderen Technik beseitigt? Wird die Überwachung mittels der verschiedenen Techniken von den Überwachten schon als umfassend wahrgenommen? Lassen sich panoptisch wirkende Überwachungstechniken überhaupt mit der Idee von Demokratie verbinden?

Die wichtigste Frage aber bleibt: Wollen wir in einer Normalisierungs- oder Kontrollgesellschaft leben?

6. Quellen

AK Vorratsdatenspeicherung (2007):

Vorratsdatenspeicherung: Das Internet trauert um das

Telekommunikationsgeheimnis.

<<http://www.vorratsdatenspeicherung.de/content/view/158/79/lang,de>> Zugriff:

10.4.2010

AK Vorratsdatenspeicherung (2007):

Pro und Contra Vorratsdatenspeicherung.

<<http://www.vorratsdatenspeicherung.de/content/view/83/87/lang,de/>> Zugriff:

12.4.2010

Albrecht, Hans-Jörg (2008):

Kosten und Nutzen technisierter Überwachung. In: Gaycken, Sandro / Kurz, Constanze (Hrsg.) (2008): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: Transcript. S. 129 - 148

Albrecht, Hans-Jörg / Grafe, Adina / Kilchling, Michael (2008):

Rechtswirklichkeit der Auskunftserteilung über

Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO.

Forschungsbericht im Auftrag des Bundesministeriums der Justiz.

<[http://www.bmj.bund.de/files/-/3045/MPI-GA-2008-02-](http://www.bmj.bund.de/files/-/3045/MPI-GA-2008-02-13%20Endfassung.pdf)

[13%20Endfassung.pdf](http://www.bmj.bund.de/files/-/3045/MPI-GA-2008-02-13%20Endfassung.pdf)> Zugriff: 8.4.2010

Alvaro, Alexander (2006):

Die Richtlinie zur Vorratsdatenspeicherung. In: DANA – Datenschutz

Nachrichten, 2/2006, S. 52 - 55

Bogdal, Klaus-Michael (2008):

Überwachen und Strafen. In: Kammler, Clemens / Parr, Rolf / Schneider, Ulrich Johannes (Hrsg.) (2008): Foucault Handbuch. Leben – Werk – Wirkung.

Stuttgart: J.B. Metzler. S. 68 – 80

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit:

Vorratsdatenspeicherung.

<http://www.bfdi.bund.de/cln_007/nn_533578/DE/Schwerpunkte/Vorratsdaten/Artikel/Vorratsdatenspeicherung.html> Zugriff: 5.4.2010

Bundesgesetzblatt (2007):

Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG. In: Bundesgesetzblatt, Jahrgang 2007 Teil I, Nr. 70. Bonn: Bundesanzeiger Verlag. S. 3198 - 3211

Bundesverfassungsgericht (2010):

Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß.

<<http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html>>

Zugriff: 13.4.2010

Deutscher Bundestag (2008):

Drucksache 16/11139. Auswirkungen der Vorratsdatenspeicherung.

<<http://dip21.bundestag.de/dip21/btd/16/111/1611139.pdf>> Zugriff: 6.4.2010

Engling, Dirk (2008):

Vorratsdatenspeicherung. In: Gaycken, Sandro / Kurz, Constanze (Hrsg.) (2008): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: Transcript. S. 67 - 78

Forsa (2008):

Meinungen der Bundesbürger zur Vorratsdatenspeicherung.

<http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf> Zugriff: 4.4.2010

Foucault, Michel (1994):

Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt/Main: Suhrkamp

Golem.de (2007):

Richterverband: Vorratsdatenspeicherung bringt 0,006 Prozent. Bundesregierung steuert auf ein Desaster zu. <<http://www.golem.de/0707/53525.html>> Zugriff: 15.4.2010

Grafe, Adina (2008):

Die Auskunftserteilung über Verkehrsdaten nach §§ 100g, 100h StPO – Staatliche Kontrolle unter Mitwirkung Privater. <<http://www.freidok.uni-freiburg.de/volltexte/6085/pdf/Verkehrsdaten.pdf>> Zugriff: 14.4.2010

Haggerty, Kevin D. (2006):

Tear down the walls: on demolishing the panopticon. In: Lyon, David (Hg.) (2006): *Theorizing Surveillance. The panopticon and beyond*. Portland, Oregon: Willian Publishing. S. 23 -46

Heise Online (2009):

Rumänisches Verfassungsgericht untersagt Vorratsdatenspeicherung. <<http://www.heise.de/newsticker/meldung/Rumaenisches-Verfassungsgericht-untersagt-Vorratsdatenspeicherung-821137.html>> Zugriff: 12.4.2010

Heise Online (2010a):

EU will Datenspeicherungsrichtlinie überprüfen. <<http://www.heise.de/newsticker/meldung/EU-will-Datenspeicherungsrichtlinie-ueberpruefen-945936.html>> Zugriff: 12.4.2010

Heise Online (2010b):

EU will Pflicht zur Vorratsdatenspeicherung neu prüfen. <<http://www.heise.de/newsticker/meldung/EU-will-Pflicht-zur-Vorratsdatenspeicherung-neu-pruefen-942207.html>> Zugriff: 12.4.2010

Heise Online (2010c):

Vorratsdatenspeicherung: Zivilgesellschaft fordert endgültige Abschaffung. <<http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-Zivilgesellschaft-fordert-endgueltige-Abschaffung-981313.html>> Zugriff: 20.4.2010

Heise Online (2010d):

Polizeipräsident: Urteil zur Vorratsdatenspeicherung bremst Polizei aus. <<http://www.heise.de/newsticker/meldung/Polizeipraesident-Urteil-zur-Vorratsdatenspeicherung-bremst-Polizei-aus-962935.html>> 12.4.2010

Hickethier, Knut (2003):

Einführung in die Medienwissenschaft. Stuttgart: J. B. Metzler

Kremp, Stefan (2010)

Bürgerrechtler starten Kampagne gegen neue Vorratsdatenspeicherung.

<<http://www.heise.de/newsticker/meldung/Buergerrechtler-starten-Kampagne-gegen-neue-Vorratsdatenspeicherung-949526.html>> Zugriff: 12.4.2010

Kremp, Stefan (2010a):

Schweden widersetzt sich der Vorratsdatenspeicherung.

<<http://www.heise.de/newsticker/meldung/Schweden-widersetzt-sich-der-Vorratsdatenspeicherung-923756.html>> Zugriff: 12.4.2010

Kremp, Stefan (2010b):

Justizministerin hält Vorratsdatenspeicherung für verzichtbar.

<<http://www.heise.de/newsticker/meldung/Justizministerin-haelt-Vorratsdatenspeicherung-fuer-verzichtbar-959955.html>> Zugriff: 12.4.2010

Kubieziel, Jens (2007):

Anonym im Netz. Techniken der digitalen Bewegungsfreiheit. München: Open Source Press

Kurz, Constanze / Rieger, Frank (2009):

Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung.

<<http://ccc.de/de/vds/VDSfinal18.pdf>> Zugriff: 14.4.2010

Lyon, David (2006):

Bentham's Panopticon: From Moral Architecture to Electronic Surveillance. In: Norris, Clive / Wilson, Dean (Hrsg.) (2006): Surveillance, Crime and Social Control. Aldershot: Ashgate

Maras, Marie-Helen (2009):

From targeted to mass surveillance: is the EU Data Retention Directive a necessary measure or an unjustified threat to privacy? In: Goold, Benjamin J. / Neyland, Daniel (Hrsg.) (2009): New Directions in Surveillance and Privacy. Cullompton: Wallan

Ruoff, Michael (2009):

Foucault-Lexikon. Paderborn: Wilhelm Fink

Schaar, Peter (2007):

Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft.

München: Bertelsmann

Schaar, Peter (2008):

Stellungnahme zu den Verfassungsbeschwerden

1 BvR 256/08

1 BvR 263/08

1 BvR 586/08

gegen die Regelungen zur Vorratsdatenspeicherung im Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007.

<<http://www.bfdi.bund.de/cae/servlet/contentblob/952736/publicationFile/62210/StellungnahmeVorratsdaten311008.pdf>> Zugriff: 12.4.2010

Schaar, Peter (2009):

Verfassungsbeschwerden gegen die Regelung zur Vorratsdatenspeicherung im Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007. Stellungnahme zum Fragenkatalog.

<<http://www.bfdi.bund.de/cae/servlet/contentblob/952738/publicationFile/62213/StellungnahmeVorratsdaten100609.pdf>> Zugriff: 12.4.2010

Schneider, Adrian (2010):

BVerfG zu Vorratsdatenspeicherung: Was geht, was geht nicht?

<<http://www.telemedicus.info/article/1663-BVerfG-zu-Vorratsdatenspeicherung-Was-geht,-was-geht-nicht.html>> Zugriff: 17.4.2010

Schröder, Burkhard (2008):

Bitte bevorraten Sie sich. <<http://www.heise.de/tp/r4/artikel/27/27544/1.html>>

Zugriff: 15.4.2010

Seier, Andrea (2001):

Macht. In: Kleiner, Marcus S. (Hg.) (2001): Michel Foucault. Eine Einführung in sein Denken. Frankfurt/Main: Campus Verlag. S. 90 - 107

Spitz, Malte:

Antwort der Bundesnetzagentur auf Auskunftsanspruch bei der
Vorratsdatenspeicherung. <<http://www.malte-spitz.de/suchen/2907405.html>>
Zugriff: 16.4.2010

Stern (2007):

stern-Umfrage: Bundesbürger mehrheitlich gegen Schäubles Sicherheitspläne.
<<http://www.stern.de/presse/vorab/590457.html>> Zugriff: 8.4.2010

Vetter, Udo (2010):

Anonym über UMTS.
<<http://www.lawblog.de/index.php/archives/2010/04/19/anonym-uber-umts/>>
Zugriff: 20.4.2010

Wolf, Burkhardt (2008):

Panoptismus. In: Kammler, Clemens / Parr, Rolf / Schneider, Ulrich Johannes
(Hrsg.) (2008): Foucault Handbuch. Leben – Werk – Wirkung. Stuttgart: J.B.
Metzler. S. 279 – 284

Ziercke, Jörg (2007):

Polizei in der digitalen Welt.
<http://www.bka.de/kriminalwissenschaften/herbsttagung/2007/langfassung_ziercke.pdf> Zugriff: 14.4.2010