Freie Universität Berlin
Fachbereich Politik- und Sozialwissenschaften
Otto-Suhr-Institut für Politikwissenschaft
SS 2006

HS 15332: „Berlin – sichere Stadt?“
Dozent: Norbert Pütter

Hausarbeit

Die neue „Sicherheit“: Vorratsdatenspeicherung als Ausdruck einer präventiven Wende in der Innen- und Sicherheitspolitik

Martin Schauerhammer

Inhaltsverzeichnis

1 Vorbetrachtung

"In dem ein oder anderen Fall ist das BVerfG der Meinung das sei nicht mit der Verfassung vereinbar. Ich räume ein, das ist nicht immer vorhersehbar. Ich habe auch das Grundrecht auf informationelle Selbstbestimmung im Grundgesetz bisher nicht gefunden."

August Hanning, Staatssekretär im Bundesministerium des Inneren[1]

Betrachtet man die Innen- und Sicherheitspolitik in der Bundesrepublik Deutschland der letzten Jahre, so lässt sich feststellen, dass es einen Paradigmenwechsel in der Politik, sowie einen Sinneswandel in der Bevölkerung gegeben hat.

Ersterer drückt sich in einer Innenpolitik aus, die in immer stärkerem Maße eine präventive Prägung erfährt, sich also schon vor einer vollzogenen Straftat in staatlichen Handlungen zur Gefahrenabwehr manifestiert. Diese staatlichen Handlungen sind zum Teil mit tiefen Eingriffen in die Bürgerrechte verbunden – so etwa im Bereich der Telekommunikations- und Videoüberwachung, durch verschärfte Pass- und Ausweisgesetze, dem Einsatz von biometrischen Daten, oder aktuell insbesondere durch die geplante Gesetzgebung zur Vorratsdatenspeicherung von Telekommunikationsverbindungen[2].

Ein Sinneswandel in der Bevölkerung lässt sich unter anderem an dem Desinteresse und einem kaum vorhanden Problembewusstsein erkennen, insbesondere wenn man den historischen Vergleich zum Volkszählungsurteil und den diesem vorhergehenden massiven Protesten von Bürgerrechtlern und Intellektuellen heranzieht[3]. Regte sich in den 70er und 80er Jahren noch reger Widerstand gegen staatliche Datenerhebungen ohne konkrete Zielbestimmung und den damit verbundenen Einschränkungen von Bürgerrechten, so ist spätestens seit dem Ende der Blockkonfrontation ein neuer Trend zu beobachten: Mit steigenden persönlichen Risiken – im wissenschaftlichen Diskurs wird von dem Übergang von der postmodernen zur Risikogesellschaft[4] ausgegangen – steigt auch das Sicherheitsbedürfnis der Bevölkerung.
In einer Welt, die für den Einzelnen immer überschaubarer wird, deren Risiken nicht mehr kalkulierbar erscheinen, in der die Unwägbarkeiten von Umweltverschmutzung, Demographie, Reichtumsschere,

1 August Hanning, Staatssekretär im Bundesministerium des Inneren in Tagesschau: *Alltag Überwachung,* http://213.200.64.229/tagesschau/mp3/misc/alltag-ueberwachung_komplett.mp4 abgerufen 03.04.2007

2 vgl. *Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*, http://www.vorratsdatenspeicherung.de/images/RefE-2006-11-27.pdf abgerufenen 05.04.2007

3 So zitiert der Guardian das jährliche British Social Attitudes Survey dem zufolge eine überwältigende Mehrheit der Menschen ist bereit, weitere Freiheiten im Kampf gegen den Terrorismus aufzugeben. The Guardian, 24.Januar 2007: http://www.guardian.co.uk/terrorism/story/0,,1997283,00.html abgerufen: 20.03.2007

4 vgl. Ulrich Beck: *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Suhrkamp, Frankfurt a.M. 1986

wirtschaftliche Unsicherheit durch globale und damit höchst flexible Märkte zunehmen und in der tradierte gesellschaftliche Bindungen gegenüber der allgemeinen Individualisierung[5] zurücktreten, steigen die Bedürfnisse des Einzelnen nach Sicherheit.

Seit Jahren sind Bürgerrechtler und Datenschützer darum bemüht, die für freiheitlich-demokratische Rechtsstaaten konstitutiven Bürgerrechte, gegen welche nicht erst seit dem Aufkommen des neuzeitlichen global agierenden Terrorismus von Seiten der Politik argumentiert wird, in Stellung zu bringen, und deren - für jeden einzelnen Bürger fundamentalen Vorzüge - gegenüber einer mutmaßlich „sicheren Gesellschaft“ in der Öffentlichkeit zu positionieren. Bisher ist dieses Bemühen von nur mäßigem Erfolg geprägt[6].

Diese Arbeit beschäftigt sich mit der aktuellsten Blüte des neuen sicherheitspolitischen Paradigmas, dem in Bezug auf die durch das deutsche Grundgesetz und die Europäische Menschenrechtskonvention garantierten Freiheits- und Bürgerrechten wohl bisher einschneidensten Gesetzgebungsverfahren zur Vorratsdatenspeicherung von Telekommunikationsdaten. Es ist geplant, das Kommunikationsverhalten aller rund 450 Mio. in Europa lebenden Bürger zu erfassen und für eine Zeit von zwischen 6 und 24 Monaten zu speichern. Dabei sollen die Verkehrsdaten – also jene Daten, die Aufschluss darüber geben, wer wann mit wem über das Internet, Festnetztelefon und Mobiltelefonie mit wem wie lange kommuniziert hat – verdachtsunabhängig gespeichert werden.

Im Zentrum der Arbeit soll der Fragestellung nachgegangen werden, welche Implikationen sich sowohl für die Gesellschaft als solche, als auch den politisch-administrativen Apparat unser freiheitlich-demokratischen Grundordnung aus dem im Verlauf der Arbeit diagnostizierten präventiven Wandel in der Innen- und Sicherheitspolitik ergeben. Dies soll anhand des aktuellen Referentenentwurfs zur Vorratsdatenspeicherung, sollte er politisch durchgesetzt werden und juristisch Bestand haben[7], problematisiert werden.
Wie tiefgreifend ist also der mit einem solchen Gesetz verbundene Wandel der freiheitlich-demokratischen Grundordnung: Handelt es sich wirklich um den von Datenschützern prognostizierten Dammbruch oder ist das Gesetz passgenau auf die Bekämpfung schwerer Verbrechen

5 Als Individualisierung wird hier der Prozess der Ablösung industrie-gesellschaftlichen Lebensformen („Normalarbeitsverhältnisse“, „Normalbiographie“) durch die postindustriellen Werte von Selbstbestimmung und Selbstverwirklichung bezeichnet, der allerdings auch Selbstverantwortung und die hiermit verbundenen Risiken mit einschließt.

6 So auch das Fazit des 22. Kongresses des Chaos Computer Clubs, nachzulesen bei Heise: *22C3: "Wir haben den Krieg verloren"*, http://www.heise.de/newsticker/meldung/67796 abgerufenen 05.04.2007

7 Auf europäischer Ebene ist bereits eine Nichtigkeitsklage Irlands anhängig, die sich gegen die auch dem deutschen Referentenentwurf zugrunde liegende Richtlinie richtet. In Deutschland wurde bereits angekündigt, dass gegen eine Vorratsdatenspeicherung Verfassungsbeschwerde durch Datenschützer eingereicht werden wird.

zugeschnitten? Welche Anwendungsgebiete und Implikationen ergeben sich für die deutschen Strafverfolgungsbehörden? Welche Perspektive folgt, wenn andere Entwicklungen im Bereich der Strafverfolgung wie Videoüberwachung, Erfassung von KfZ-Kennzeichen in Betracht gezogen werden?

Ich werde zunächst in einem historischen Abriss die Entstehungsgeschichte der geplanten Gesetzgebung aufzeigen, dabei werde ich sowohl auf bundespolitische und länderpolitische Begründungszusammenhänge, aber insbesondere auch auf die europäische und internationale Dimension des Verfahrens eingehen.
Hieran schließt sich eine Darstellung der eigentlichen Gesetzgebung auf Grundlage des vorliegenden Referentenentwurfes an. Es wird zu zeigen sein, ob und in welcher Breite dieses Gesetz die Grundlagen des freiheitlich-demokratischen Rechtsstaates, wie er durch das deutsche Grundgesetz angelegt ist, unterminiert.
Im Anschluss hieran werde ich erörtern, welche Auswirkungen durch die Vorratsdatenspeicherung auf Landes-, Bundes-, sowie EU-Ebene mit Bezug auf Grund- und Bürgerrechte haben kann. Hierbei werde ich ähnlich gelagerte Gesetzgebungen der letzten Jahre einbeziehen, um die Chancen und Risiken, die sich in der Zusammenschau dieser auf Prävention basierenden Sicherheitsstrategie zeigen, zu verdeutlichen und gegeneinander abzuwägen.
Abschließend werde ich die gemachten Beoachtungen zu einem Fazit zusammenziehen, das die aktuelle Sicherheitspolitik kritisch hinterfargt.

2 Die Vorratsdatenspeicherung (in Deutschland) – Ein Rückblick

Bestrebungen, eine Vorratsdatenspeicherung einzuführen gibt es sowohl auf deutscher als auch europäischer Ebene schon lange. Als ausschlaggebendes Ereignis kann wohl der Terroranschlag des 11. Septembers 2001 in den USA angenommen werden, auch wenn dieser auf politischer Ebene vorrangig eher als Argument zur Notwendigkeit eines solchen Gesetzes genutzt wurde, ohne die Wirksamkeit einer solchen Maßnahme zu belegen. Bisher ist nicht erwiesen, ob eine Speicherung von Verkehrsdaten zu einer erhöhten Aufklärungsquote oder gar zur Verhinderung von Terroranschlägen und anderen schweren Straftaten führen kann.

2.1 Das Cybercrime Abkommen

Die am 23. November 2001 vom Europarat beschlossene „Convention on Cybercrime“[8] kann auf europäischer Ebene als erster Schritt in Richtung einer europaweiten Vorratsdatenspeicherung angesehen werden. Mit der weltweiten Verbreitung und Nutzung der neuen Telekommunikationstechnologien hat auch das Ausmaß an mit ihnen begangen Straftaten zugenommen[9].

Als Erklärung der wachsenden registrierten Straftaten mit Bezug zu modernen Kommunikationstechnologien können verschiedene Ansätze in Betracht kommen. So sind etwa die Verbreitung und der Konsum von kinderpornographischen Inhalten über das Internet um ein vielfaches einfacher zu realisieren, als in der „offline“-Welt. Zudem vermittelt das weltweite Datennetz eine gefühlte Anonymität, die sich bei ausreichendem technischen Wissen durch die Nutzung von weiteren Hilfsmitteln wie Anonymisierungsdiensten[10] in eine echte Anonymität[11] – zumindest aber Pseudonymität[12] verwandeln lässt.

Durch diese Eigenschaften ist das Internet eine ideale Plattform für eine Vielzahl von Rechtsverstößen – so etwa die Verbreitung von urheberrechtlich geschützten Werken, für Kreditkarten- und Internetbetrug, für die Verbreitung von rechtsradikalen und menschenverachtenden Inhalten oder aber zur Vorbereitung von terroristischen Anschlägen. Auf der anderen Seite haben sich die neuen Technologien mittlerweile zu Mainstream-Medien der Kommunikation[13]

8 Deutscher Volltext der „*Convention on Cybercrime*“: http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm abgerufen 20.03.2007

9 vgl. hierzu *Polizeiliche Kriminalstatistik 2005* sowie Pressemitteilung der Berliner Senatsverwaltung für Justiz: *Deutlicher Zuwachs an Internet-Straftaten: Bericht der Staatsanwaltschaft zur Entwicklung der Verfahrensdaten*, Berlin 19.12.2005, http://www.berlin.de/sen/justiz/presse/archiv/20051219.26103.html abgerufenen 19.03.2007

10 Einen guten Überblick findet man bei Kai Raven: *Anleitungen und Einführungen*, http://hp.kairaven.de/misc/anleitung.html abgerufen am 05.04.2007

11 Anonymität bedeutet, dass ein Benutzer nicht seiner realen Identität zugeordnet werden kann. vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI): *Was ist Anonymität?*, http://www.bsi.de/literat/anonym/wasist.htm abgerufenen am 04.04.2007

12 Pseudonymität bedeutet, dass ein Benutzer, der unter einem Pseudonym handelt, einen Dienst nutzen kann ohne seine Identität preiszugeben.

13 Von 1997 bis 2006 stieg der Anteil der Internet-Nutzer in Deutschland von 6,5 Prozent auf 59,5 Prozent. 38,6 Millionen bundesdeutsche

entwickelt, so dass es in der Natur der Sache liegt, dass mit einer stärkeren allgemeinen Verbreitung und Nutzung der neuen Kommunikationsmedien auch die Zahl derer zunimmt, die die neuen Kommunikationsformen für kriminelle Ziele missbrauchen.

Legt man allerdings die Zahlen der Polizeilichen Kriminalstatistik 2005 zugrunde, sind die mittels Telekommunikationstechnik begangene Straftaten im Vergleich zu anderen Formen der Kriminalität zu vernachlässigen. So wurden im Jahr 2005 62.186 Fälle von Computerkriminalität ermittelt, was im Vergleich zu den 6.391.715 erfassten Straftaten in Deutschland als gering anzusehen ist[14]. Auch wenn die als „Straftaten mit Tatmittel Internet“ ausgewiesenen Daten zugrunde gelegt werden, ergibt sich kein anderes Bild (118.036 Straftaten mit Internetbezug im Vergleich zu 5.107.892 gesamt[15]), so dass der Anteil von mittels modernen Kommunikationsformen begangener Straftaten wohl insgesamt überschätzt oder vielmehr politisch gewollt überhöht dargestellt wird.

Durch das Cybercrime-Abkommen, das seit 2004 in Kraft ist und das neben den Mitgliedern des Europarates von den USA, Kanada, Japan und Südafrika unterzeichnet wurde, soll nun eine bessere Bekämpfung dieser Straftaten und die Ermittlung der durch die internationalen Kommunikationsnetze nicht mehr oder nur schwer geographisch lokalisierbaren Täter gewährleisten[16]. Hierfür werden neue Formen und effektive Wege der Zusammenarbeit in der Strafverfolgung über nationalstaatliche Grenzen hinweg ermöglicht.

So können nach Artikel 16 des Abkommens ausländische Strafverfolgungsbehörden durch ein Amtshilfeersuchen an einen anderen Staat das Einfrieren von Kommunikationsdaten über einen Zeitraum von 90 Tagen bei Dienstanbietern ohne richterlichen Beschluss erwirkt werden. Aber nicht nur das Einfrieren von Daten ist vorgesehen, auch die Weitergabe an Drtittstaaten wird ermöglicht. So haben die Vertragsstaaten dafür Sorge zu tragen, *daß „dass Verkehrsdaten [...] umgehend an die zuständige Behörde der Vertragspartei [...] weitergegeben werden [können] [...]“*[17].

Im Artikel 20 werden die Unterzeichnerstaaten dazu angehalten, Gesetze zu erlassen, die die Anbieter von Internetzugängen dazu zu verpflichten, die Möglichkeit von Datensammlungen in Echtzeit zu schaffen. So sollen Dienstanbieter verpflichtet werden können, *„Verkehrsdaten durch Anwendung technischer Mittel [...] in Echtzeit zu erheben oder aufzuzeichnen [...]“*.

Erwachsene sind inzwischen online. vgl. ARD/ZDF-Online-Studie 2006 zur Internetnutzung, http://www.ard-werbung.de/showfile.phtml/eimeren.pdf?foid=17746 abgerufenen am 02.04.2007

14 vgl. Bundesministerium des Inneren: *Polizeiliche Kriminalstatistik 2005, S.36f*

15 ebd. S.8

16 vgl. hierzu Marco Gercke: *Analyse des Umsetzungsbedarfs der Cybercrime Konvention: Umsetzung im Bereich des materiellen Strafrechts*, in MMR 2004 Heft 11, S. 728ff sowie Marco Gercke: *Analyse des Umsetzungsbedarfs der Cybercrime Konvention: Umsetzung im Bereich des Strafverfahrensrechts*, MMR 2004 Heft 12, S. 801ff

17 vgl. Artikel 17 der „*Convention on Cybercrime*“

Die Umsetzung der genannten Artikel unterliegt den in Artikel 15 der Konvention bezeichneten Schranken, wobei insbesondere die Europäische Menschenrechtskonvention sowie die UN-Charta der Menschenrechte genannt werden.

Auch wenn die „Convention on Cybercrime“ noch nicht in allen Ländern und insbesondere nicht in Deutschland ratifiziert wurde[18], so zeigt sie doch auf, dass ein internationaler Umsetzungsdruck zur Verwirklichung der im Cybercrime-Abkommen formulierten Strafverfolgungsinstrumente besteht, der letzten Endes neben weiteren Begründungszusammenhängen[19] zum aktuellen Referentenentwurf zur „Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ in Deutschland geführt hat. Zwar ist der „Convention on Cybercrime“ keine Verpflichtung zur Einführung einer generellen Vorratsdatenspeicherng zu entnehmen, einige dort formulierten Verfahren wie das der Datenerfassung in Echtzeit wurden aber in Deutschland bereits umgesetzt. So dient die Telekommunikations-Überwachungs-Verordnung eben jenem im Abkommen formulierten Verfahren des „Quick-Freeze“, dem verdachtsabhängigen Speichern von Verbindungs- und Inhaltsdaten[20].

Wir haben gesehen, dass es auf internationaler Ebene Abkommen gibt, die bereits Elemente der geplanten Vorratsdatenspeicherung enthalten. Die „Convention on Cybercrime“ führt aber insbesondere vor Augen, dass sich die politischen Argumente für eine stärkere Strafverfolgung im Bereich der mittels Kommunikationstechnologien begangener Straftaten beliebig austauschen lassen, je nach aktueller Gefahrenlage werden internationaler Terrorismus, organisierte Kriminalität oder Kinderpornographie, sowie verschiedene Ausprägungen politischer Radikalisierung als Gründe eines Eingriffes in garantierte Grundrechte durch die politischen Akteure angebracht.

Auf internationaler Ebene ist die fehlende strikte Eingrenzung der Anlässe von Eingriffen sowie der behördlichen Zusammenarbeit besonders kritisch zu bewerten, da hier eine Kontrollinstanz wie die parlamentarische fehlt. Die klassische Frage, die hier gestellt werden muss fragt nach dem Überwacher des überstaatlichen Überwachers, der im Abkommen nicht benannt wird. Vielmehr wird Bezug genommen auf die allgemein anerkannten Grund- und Menschenrechte: eine schwache Lösung im Vergleich zur Eingriffstiefe die die Konvention formuliert.

Welche Bestrebungen hat es in der Folge auf nationalstaatlicher Ebene in Deutschland für eine Vorratsdatenspeicherung gegeben und welche

18 vgl. zum Stand der Ratifizierung: Convention on Cybercrime CETS No.: 185, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=8/4/2006&CL=ENG abgerufenen am 05.04.2007

19 Gemeint sind die steigenden Unsicherheiten aufgrund ökologischer, wirtschaftlicher, sozialer oder politischer Verwefungen und der politischen motivierten Notwendigkeit, Handlungsfähigkeit unter Beweis zu stellen.

20 vgl. hierzu Informationen des Bundesministerium für Wirtschaft und Technologie zur Telekommunikations-Überwachungsverordnung (TKÜV), http://www.bmwi.de/Navigation/Wirtschaft/telekommunikationundpost,did=6018.html abgerufenen am 02.04.2007

Begründungen wurden von politischer Ebene angeführt, um eine präventive Erfassung von Kommunikationsdaten zu ermöglichen?

2.2 Die Bundesratsinitiative von 2002

Vor den Terroranschlägen des 11. September wurde von den Innenministern vor allem die Bekämpfung der organisierten Kriminalität und die Verfolgung schwerer Straftaten für eine Verschärfung von Gesetzen ins Feld geführt.

So auch bei der vom Land Niedersachsen im März 2002 in den Bundesrat eingebrachten Gesetzesinitiative „Gesetzesentwurf zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Kindesmißbrauchs und der Vollstreckung freiheitsentziehender Sanktionen“[21]. In deren Begründung es heißt: *„Mit flächendeckender Verbreitung des Internets entwickelt sich der sexuelle Missbrauch von Kindern immer mehr zu einem lohnenden Geschäft mit erheblich erleichterten und vor allem anonymen Zugangs- und Kontaktmöglichkeiten für (pädophile) Kriminelle.*“ Da sich „[*die] Überwachung der Telekommunikation [...] als ein effizientes Mittel der Strafverfolgung erwiesen [...]*“[22] habe, wird diese als adäquates Mittel erachtet, den mutmaßlich steigenden Zahlen des sexuellen Missbrauchs von Kindern entgegen zu wirken.

Um eine bessere Strafverfolgung- und Vorbeugung im Bereich des sexuellen Missbrauchs zu gewährleisten, sollte der „bisherige, unbefriedigende“ Gesetzeszustand erweitert werden. So sollten die kommerziellen Anbieter von Telekommunikationszugängen zur „*Vorratsspeicherung für Zwecke der Strafverfolgung und der Gefahrenabwehr und für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes*“[23] verpflichtet werden. Welche Daten hiermit erfasst werden sollten, wurde nicht klar angegeben, §89 Telekommunikationsgesetz (TKG) geht hier von „personenbezogenen Daten“ aus. In der Zusammenschau mit dem ebenfalls erweiterten §6 Teledienstedatenschutzgesetz (TDDSG) werden durch die Vorratsdatenspeicherung aber auf jeden Fall die „*Bestands-, Nutzungs- und Abrechnungsdaten*“ erfasst. Der neue §6a TDDSG der Gesetzesinitiative verpflichtet die Bundesregierung zum Erlassen einer entsprechenden Rechtsverordnung:

„Die Bundesregierung erlässt für Diensteanbieter durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften zur Vorratsspeicherung für die Zwecke der Strafverfolgung und der Gefahrenabwehr und für die Erfüllung der gesetzlichen Aufgaben der

21 vgl. Bundesrats-Drucksache 275/02 S.1

22 vgl. ebd. S.2

23 vgl. ebd. S.4

Verfassungsschutzbehörden des Bundes und der Länder, des Bundes nachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes. Dabei sind Mindestfristen für die Speicherung von Bestands-, Nutzungs- und Abrechnungsdaten festzulegen und insgesamt die berechtigten Interessen der Diensteanbieter, der Betroffenen und die Erfordernisse effektiver Strafverfolgung und Gefahrenabwehr sowie der effektiven Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes zu berücksichtigen."

Beachtenswert hierbei ist, dass hier als Ziel der Datenerfassung nur Rede von Zwecken der „Strafverfolgung und Gefahrenabwehr" ist, welche Straftaten hierdurch erfasst werden und welchen Gefahren begegnet werden soll wird der Form der Rechtsverordnungung überlassen. Somit findet eine explizite Zweckbindung, wie sie bei solch erheblichen Grundrechtseingriffen laut Grundgesetz verbindlich wäre[24] nicht statt.

Die durch den Rechtsausschuss des Bundesrates erarbeitete Beschlussfassung des Gesetzesentwurfes wurde am 31. Mai 2002 durch den Bundesrat verabschiedet und der Bundesregierung zur Stellungnahme vorgelegt. Die Bundesregierung hat den Gesetzesentwurf mit seiner Stellungnahme[25] am 16. Juli 2002 dem Bundestag zur Entscheidung vorgelegt.

Die Stellungnahme der Bundesregierung fällt zu diesem Zeitpunkt verhalten aus: Zum einen wird betont, dass es ein natürliches Spannungsverhältnis zwischen den durch die Maßnahmen der Gesetzesinitiative eingeschränkten Bürgerrechten und dem staatlichen Ordnungsauftrag im Sinne der Schaffung von Sicherheit gäbe. So sei die Bundesregierung bestrebt, einen „angemessenen Interessenausgleich herbeizuführen, der das wichtige öffentliche Interesse an einer effektiven Strafverfolgung, insbesondere an einer erfolgreichen und schnellen Aufklärung schwerer Straftaten, mit den Grundrechten der Betroffenen in ein ausgewogenes Verhältnis bringt"[26]. Weiterhin wird angeführt, dass der Entwurf des Bundesrates die für die Einführung einer solchen Regelung erforderliche Abwägung der verschiedenen Rechtsgüter nicht erkennen lasse. Insgesamt wird die Gesetzesinitiative des Bundesrates zur Vorratsdatenspeicherung damit mit Verweis auf die betroffenen Grundrechte und das Gebot der Verhältnismäßigkeit durch die Bundesregierung abgelehnt.

Damit war die Einführung der Vorratsdatenspeicherung in Deutschland

24 So Urteilte das BVerfG zur Rechtmäßigkeit von Grundrechtseingriffen (hier Rasterfahndung): „Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht." vgl. BVerfG, Beschluss vom 4. 4. 2006 - 1 BvR 518/02 Abs. 137

25 vgl. Bundestags-Drucksache 14/9801

26 vgl. ebd S.15

in dieser Legislaturperiode zunächst gescheitert, die Gesetzesvorlage wurde durch die Konstituierung des 15. Deutschen Bundestages am 17. Oktober 2002 durch den Grundsatz der Diskontinuität[27] erfasst und war damit nichtig.

Jedoch begannen sich auf europäischer Ebene bereits die Konturen eines Prozesses zur Schaffung eines gemeinsamen Rechtsrahmens für eine Vorratsdatenspeicherung von Kommunikationsdaten heraus zu bilden.

2.3 Der Werdegang der EU-Richtlinie 2006/24/EG[28]

Mit der Ratspräsidentschaft des Königreichs Dänemark 2002 hat die Thematik der Vorratsdatenspeicherung eindeutig und durchgreifend die europäische Ebene erreicht. So legt das Königreich Dänemark im August einen ersten Entwurf für einen Rahmenbeschluss zur Vorratsdatenspeicherung vor, der allerdings zu diesem Zeitpunkt im Rat keine Mehrheit findet. Dort heißt es, es seien „schon in nächster Zukunft bindende Regeln für die Angleichung der Vorschriften der Mitgliedstaaten über die Pflicht der Telekommunikationsbetreiber, Telekommunikationsdaten aufzubewahren, festzulegen, damit sichergestellt ist, dass diese Daten verfügbar sind, wenn diese für strafrechtliche Ermittlungen von Bedeutung sind“[29].

Mit den Bombenanschlägen vom 11. März 2004 auf vier Regionalzüge in Madrid erreicht der mutmaßlich international agierende Terrorismus endgültig den Boden Europas und erhöht den Handlungsdruck auf die politischen Verantwortungsträger, sowohl auf europäischer als auch nationalstaatlicher Ebene.

Den ersten Bemühungen für eine Durchsetzung der Vorratsdatenspeicherung auf Grundlage der dritten Säule (Zusammenarbeit in der Justiz- und Innenpolitik) des EU-Vertragswerks folgen weitere Entwürfe für Rahmenbeschlüsse. So bringen im April 2004 Irland, Schweden und Frankreich einen solchen in den Rat der Euroäischen Union ein. Unter niederländischer Ratspräsidentschaft wird dieser Entwurf überarbeitet und bringt an einigen Stellen Entlastungen für die von einer Vorratsdatenspeicherung betroffenen Wirtschaftsunternehmen. So werden die einzubeziehenden Daten begrenzt und die Speicherungsfrist von 36 auf 12 Monate verkürzt.

Am 7. Juni 2005 lehnt das Europäische Parlament (EP) eine weitere Initiative der Französischen Republik, Irlands, des Königreichs

27 Alle Gesetzesvorhaben, die ein Parlament bis zum Ende seiner Wahlperiode nicht abgearbeitet hat, müssen, sofern das neu gewählte Parlament dies will, nach der Wahl neu eingebracht werden.

28 *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* , http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/oj/2006/l_105/l_10520060413de00540063.pdf abgerufenen am 18.03.2007

29 vgl. Entwurf für Schlussfolgerungen des Rates über IT-bezogene Maßnahmen im Hinblick auf die Ermittlung und Verfolgung organisierter Kriminalität, S. 3 Abs. 9, http://register.consilium.eu.int/pdf/de/02/st10/10358d2.pdf abgerufenen am 27.03.2007

Schweden und des Vereinigten Königreichs für einen Rahmenbeschluss zur Vorratsdatenspeicherung mit Verweis auf den Report[30] von Alexander Nuno Alvaro ab[31], in dem eine starke finanzielle Belastung der europäischen Telekommunikationsunternehmen belegt und Zweifel an der Vereinbarkeit von im europäischen Recht verwurzelten Grundrechten sowie am effektiven Nutzen der anfallenden Daten für die Strafverfolgung formuliert werden.

Im Jahr 2005 erfolgen weitere Anstrengungen der politischen Einigung, so hat die britische Ratspräsidentschaft dem Thema der Vorratsdatenspeicherung zu einem Projekt höchster Priorität[32] erklärt. Im Juli erscheint ein neues Positionspapier des EU-Rates, eine Einigung im Rat der Innen- und Justizminister scheint jedoch nicht denkbar, zu hoch wiegen die Bedenken von Datenschützern und Industrie. Für einen Rahmenbeschluss fehlt es an der Einstimmigkeit des Rates.

Um dem Stillstand Einhalt zu gebieten, wird im September 2005 die Kommission aktiv und unterbreitet einen Vorschlag für eine Richtlinie zur Vorratsdatenspeicherung[33], der im wesentlichen auf dem Positionspapier des Rates basiert. Mit der Nutzung des Instrumentes einer Richtlinie findet eine Verschiebung des politischen Entscheidungsprozesses von der dritten in die erste Säule des „europäischen Gebäudes“ statt.

Am 14. Dezember 2005 stimmt das Europäische Parlament der Richtlinie der Kommission trotz zahlreicher Bedenken und Protesten von Datenschützern, Unternehmern und Bürgerrechtlern zu[34].

Am 21. Februar 2006 verabschiedet der Rat der Innen- und Justizminister die Richtlinie 2006/24/EG gegen die Stimmen Irlands und der Slowakei. Hiermit erreicht die Richtlinie offiziellen Status und muss in allen Mitgliedstaaten in geltendes Recht umgesetzt werden.

Die Vorratsdatenspeicherung hat somit den Weg über die erste Säule der Europäischen Zusammenarbeit geschafft, nachdem auf Ebene der Zusammenarbeit der Justiz- und Innenminister keine Einigung für einen gemeinsamen Rahmenbeschluss gefasst werden konnte.

---

30 vgl. Bericht von Alexander Nuno Alvaro (A6-0174/2005), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0174+0+DOC+PDF+V0//DE abgerufenen am 15.03.2007

31 vgl. hierzu Plenarprotokoll des EP vom 7.Juni 2005 (P6_PV(2005)06-07)

32 vgl. European Parliament plenary debate on Data Retention: Speech by Charles Clarke, UK Secretary of State for the Home Office, 13 December 2005 , http://www.eu2005.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1115146994906&a=KArticle&aid=1134649501007&date=2005-12-13 abgerufenen am 05.04.2007

33 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM/2005/0438)

34 vgl. hierzu EP-Pressebericht zur Abstimmung - Plenarsitzung vom 14.12.2005 in Straßburg, http://www.europarl.de/presse/pressemitteilungen/quartal2005_4/PM_14122005_1 abgerufenen am 27.03.2007

2.4 Zusammenfassung

Es konnte gezeigt werden, dass die Entwicklungen zu einer Rechtsgrundlage für eine Vorratsdatenspeicherung in der Vergangenheit von verschiedenen politischen Akteuren vorangetrieben wurde. Sowohl auf internationaler und europäischer Ebene, aber ebenso im Bereich der nationalstaatlichen Politik ist im Zuge der mit der mit der Globalisierung einhergehenden, steigenden Unsicherheiten eine vermehrt auf präventive Maßnahmen der Kriminaltätsverhütung setzende sicherheitspolitische Dogmatik[35] zu erkennen.

Auf der anderen Seite führt die in Zeiten globaler Kommunikationsnetze und global agierender Kriminalität erschwerte Ausübung staatlicher Ordnungsgewalt, verbunden mit dem durch die allgemeine Globalisierung verbundenen Souveränitätsverlust für die Nationalstaaten zu einem Drang der Kooperation auf supra- und internationaler Ebene. Die Staatenwelt „[...] befinden sich in einem Prozess tief greifenden Wandels, wenn nicht gar eines revolutionär zu nennenden Umbruchs: [...] Staatsaufgaben, wie wir sie seit der Entstehung des Typus des souveränen Nationalstaates kennen, [...] vielfältige Formen der Zusammenarbeit“[36] bestimmen nunmehr das staatliche Handeln. Hierfür steht sowohl die „Convention on Cybercrime“ als auch die aktuelle EU-Richtline zur Vorratsdatenspeicherung.

3 450 Mio. EU-Bürger unter Generalverdacht – Die EU Richtlinie zur Vorratsdatenspeicherung

3.1 Inhalt der RiL 2006/24/EG

Um eine Aussage über Ausgestaltung des deutschen Referentenentwurfs zur Vorratsdatenspeicherung machen zu können, sollte zunächst ein Blick auf den Inhalt der ihm Zugrunde liegenden europäischen Richtlinie geworfen werden. Hiermit ergeben sich dann auch Schlussfolgerungen mit Hinblick auf die Vereinbarkeit des deutschen Entwurfes mit der EU-Richtlinie selbst sowie der Rechtmäßigkeit mit Bezug auf die im deutschen Grundgesetz verankerten Grundrechte und anderen für Deutschland bindende Abkommen auf europäischer und internationaler Ebene.

In der Begründung der Richtlinie wird davon ausgegangen, dass eine einheitliche Regel zur Speicherung von bei elektronischer Kommunikation entstehenden Daten für alle EU-Mitgliedstaaten

35 vgl. hierzu Sebastian Bukow: Deutschland: Mit Sicherheit weniger Freiheit über den Umweg Europa, in: Europäisierung der inneren Sicherheit : eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus, Gert-Joachim Glaeßner (Hrsg.), Wiesbaden: VS, Verlag für Sozialwissenschaft, 2005 S.57

36 Gert-Joachim Glaeßner, Astrid Lorenz: Europäisierung der inneren Sicherheit - Konzept und Begrifflichkeiten, in: Europäisierung der inneren Sicherheit : eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus, Gert-Joachim Glaeßner (Hrsg.), Wiesbaden: VS, Verlag für Sozialwissenschaft, 2005

benötigt wird, um einerseits die in den Nationalstaaten unterschiedlich geregelten Regelungen zum Vorteil des gemeinsamen Binnenmarktes zu harmonisieren und andererseits eine verbesserte Strafverfolgung durch einheitliche Instrumente in der EU zu schaffen[37].

Die zu speichernden Daten umfassen alle Verkehrs- und Standortdaten, die zur Feststellung des jeweiligen Teilnehmers oder registrierten Benutzers eines Kommunikationsvorganges erforderlich sind[38]. Ausgenommen sind Inhaltsdaten, auch wenn in der Literatur umstritten ist, ob eine Trennung von Verbindungs- und Inhaltsdaten in jedem Falle, etwa bei Email-Diensten möglich ist. Auch lassen Verbindungsdaten Rückschlüsse auf den Inhalt der Kommunikation zu, so etwa wenn von einem Bürger Kontakt mit Beratungsstellen aufgenommen wurde.

Verpflichtet zur Speicherung sind Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste sowie Betreiber von öffentlichen Kommunikationsnetzen, worunter sowohl privatwirtschaftlich geführte Unternehmen als auch freie Bürgernetze wie etwa die in vielen Städten anzutreffenden Freifunk-Initiativen[39] fallen.

Durch die Richtline erfasst werden wie bereits erwähnt alle Daten, die Aufschluss über die an einem Kommunikationsvorgang beteiligten Parteien ermöglichen und umfassen bei Telefoniediensten unter anderem gewählte Rufnummern, Dauer des Vorgangs, Name und Anschrift der beteiligten Personen, Dienstart (z.B. Sprachtelefonie, SMS[40], MMS[41]), Geräte- und Mobilteilnehmerkennungen, sowie im Falle von Mobiltelefonie die Funkzelle, in der das Mobiltelefon bei Beginn der Nutzung eines Dienste eingebucht war[42].

Bei Kommunikationsvorgängen im Internet werden e-Mail-Adressen, zugewiesene Benutzerkennungen[43], Dienstart, Beginn und Ende der Internetnutzung, sowie zugewiesene IP-Adresse[44] gespeichert.

Die Richtlinie legt eine Speicherungsdauer für die genannten Daten von zwischen 6 und 24 Monaten fest[45] und bewegt sich damit weit unter dem ursprünglichen Gedanken an eine 36monatige Speicherfrist.

Unter dem Absatz 7 „Datenschutz und Datensicherheit“ werden einige

37 vgl. Begründung der „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“, Abs. 6, 7, 11

38 vgl. Art. 1 Abs. 1 RiL 2006/24/EG

39 Die Freifunk-Bürgernetze stellen für jeden offene Netzwerkinfrastrukturen bereit, die eine weitgehend anaonyme Internetnutzung, aber auch die Nutzung viele weitere Dienste kostenlos ermöglichen. Weitere Informationen zum Freifunk-Netzwerk sind unter http://www.freifunk.net zu finden. vgl. auch Christof Autengruber: Vision und Realität Freirer Community Netze - Selbstorganisation in der Netzkultur, Magisterarbeit, Universität Salzburg, Januar 2007, http://www.dslnachpankow.de/cms/modules/PDlinks/visit.php?cid=15&lid=80 abgerufen 03.04.2007

40 Short Messaging Service (SMS): Kurznachrichten in Textform, die über Mobilfunkgeräte übertragen werden können

41 Multi Media Service (MMS): Kurznachrichten mit Multimediainhalten, wie Videos und Musik

42 vgl. Art. 5 RiL 2006/24/EG

43 Gemeint sind hier Zugangsdaten, also die vom Zugangsanbieter zugewiesene Benutzerkennung, zu der meist ein Benutzerpasswort gehört, das bei der Interneteinwahl abgefargt wird. Passwörter werden durch die Richtlinie nicht erfasst.

44 Bei der Einwahl über einen Internet Service Provider (Zugangsanbieter) bekommt der Nutzer eine eindeutige „Hausnummer“ zugewiesen. Diese bleibt über die Dauer der Interneteinwahl bestehen. An diese Nummer werden dann beim Abruf von Inhalten die Daten, wie zum Beispiel eine Internetseite, geschickt.

45 vgl. Art. 6 RiL 2006/24/EG

rudimentäre Prinzipien formuliert, die die Mitgliedsstaaten einzuhalten haben. So haben diese sicherzustellen, dass die von der Speicherungspflicht betroffenen Anbieter „Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung“ schützen. Die Kosten hierfür sind durch die Anbieter zu tragen, es findet hier also eine Inanspruchnahme Privater für die öffentliche Aufgaben – hier der Strafverfolgung – statt.

Wie wurde nun die Richtlinie durch den deutschen Gesetzgeber auf die deutschen Verhältnisse adaptiert, welche Unterschiede lassen sich festmachen und wie können diese begründet werden?

4 Die Deutsche Interpretation der EU-Richtlinie

Wie bereits in Kapitel 2 gezeigt wurde, ist der aktuelle Referentenentwurf nicht der erste Versuch, eine verdachtsunabhängige Speicherung von Kommunikationsdaten in Deutschland gesetzlich vorzuschreiben. Die ersten Versuche scheiterten jedoch an Bedenken des Bundestages bezüglich datenschutzrechtlicher Belange, zu befürchteten volkswirtschaftlichen Kosten und Zweifeln an der grundgesetzlichen Vereinbarkeit einer solchen Gesetzgebung.

Mit Hinblick auf die bisherige Ablehnung des Bundesratsentwurfs von Seiten des Bundestages soll nun untersucht werden, ob aus den bisherigen Erfahrungen Lehren auf Seiten der Politik gezogen werden konnten, ob also im aktuellen Referentenentwurf des Justizministeriums ein Umdenken im Sinne eines gestärkten Datenschutzes sowie eine Ausrichtung an den Grundsätzen der deutschen Verfassung zu erkennen ist und ob eine finanzielle Entlastung der von der Vorratsdatenspeicherung betroffenen Anbieter vorgesehen ist.

In diesem Fall wäre meine Hypothese einer neuen sicherheitspolitischen Dogmatik, die sich auf allen politischen Ebenen, angefangen bei den Innenministern der Bundesländer, über die bundesdeutsche Innenpolitik bis hin zur europäischen und internationalen Ebene zeigt und deren Zielsetzung es ist, die mit der Globalisierung steigenden Unsicherheiten durch den Ausbau von präventiven Kontrollaparaten zu begegnen, für Deutschland zunächst widerlegt.

Bei dem gegensätzlichen Fall, nämlich der einseitigen Übernahme der durch die Richtlinie formulierten Maximen oder gar der Verschärfung dieser, ist davon auszugehen, dass es sich um den von Datenschützern und Bürgerrechtlern prognostizierten Paradigmenwechsel in der Innen- und Sicherheitspolitik handelt, dessen Auswirkungen auf die freiheitlich-demokratische Grundordnung einer weiteren Untersuchung[46] bedürfen.

46 So auch Stephan Heinrich: Auf dem Weg in einen Überwachungsstaat? Informationssicherheit und Kontrolle in offenen Kommunikationsnetzen, Marburg: Tectum-Verl., 2004 S. 115f

Insbesondere die Akteurskostellation und die den Akteuren gemeinen Werte und Zielvorstellungen sind hierbei von Interesse, um zu verstehen, warum das historisch tief in den europäischen Nationalstaaten verwurzelte, auf humanistisch-freiheitlichen Idealen bauende Gesellschaftsbild immer weiter in den Hintergrund zu treten scheint.

Wie wurde also die europäische Richtlinie bisher in Deutschland im Referentenentwurf umgesetzt, hat ein Umdenken stattgefunden und wo liegen die bemerkenswerten Aspekte des deutschen Weges?

4.1 Der Referentenentwurf – Begründungen und Anforderungen

Der Referentenentwurf des Justizministeriums vom vom 27. November 2006 ist als „Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ betitelt[47]. Er soll dazu dienen, ein „harmonisches Gesamtsystem der strafprozessualen heimlichen Ermittlungsmethoden“[48] zu schaffen und verschiedenen aktuellen Urteilen des Bundesverfassungsgerichts Rechnung tragen. Nötige Anpassungen ergeben sich zudem mit Hinblick auf die in Deutschland geplante Ratifizierung der „Convention on Cybercrime“ und der europäischen Richtlinie über die Vorratsdatenspeicherung.

Die geplanten Änderungen sollen den verfassungsmäßigen Anforderungen gerecht werden. Hierzu heißt es: „*Der Gesetzentwurf soll [...] die verfahrensrechtlichen Voraussetzungen und grundrechtssichernden Ausgestaltungen der verdeckten strafprozessualen Ermittlungsmaßnahmen harmonisieren und diesen Regelungskomplex dadurch insgesamt übersichtlicher und rechtsstaatlichen Geboten entsprechend gestalten, zugleich aber auch praktischen Erfordernissen Rechnung tragen.*“[49]

Betrachtet man, was der Stellungnahme und Begründung der zu veranlassenden Gesetzesänderung folgt, so lässt sich feststellen, dass der Gesetzestext nur in einem einzigen Punkt positiver als in der europäischen Richtlinie ausfällt – den Speicherungsfristen. Hierbei orientiert sich der Entwurf am unteren Rand der Richtlinie und sieht eine 6monatige Speicherung von Verkehrsdaten vor.

Es lässt sich nicht nur inhaltlich feststellen, dass weite Teile der europäischen Richtlinie eins zu eins übernommen wurden: Sowohl Aufbau als auch Sprachgebrauch lassen schließen, dass eine tief greifende Prüfung der in der Richtlinie formulierten Vorgaben nicht

47 Bundesministeriums der Justiz: Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (RB 3 zu: 4104/11 - R5 884/2006), http://www.vorratsdatenspeicherung.de/images/RefE-2006-11-27.pdf abgerufenen am 05.04.2007

48 ebd. S.1

49 ebd S.3

stattgefunden haben kann. Mehr noch – es finden sich auch zahlreiche Verschärfungen der Richtlinie in den Gesetzesänderungen.

So werden durch den Begriff „öffentliche Kommunikationsdienste“ auch Anonymisierungsdienste einbezogen: „*Einen Telekommunikationsdienst für die Öffentlichkeit im Sinne dieser Vorschrift erbringt auch, wer einen Anonymisierungsdienst betreibt und hierbei die Ausgangskennung des Telekommunikationsnutzers durch eine andere ersetzt.*“[50]

Diese Dienste wurden zwar durch die EU-Richtlinie nicht explizit ausgeschlossen, die Einbeziehung durch die deutsche Interpretation der Richtlinie lässt aber erkennen, dass es eine Umbewertung des dem Rechtsstaat zugrunde liegenden Gedanken der Unschuldsvermutung[51] gegeben hat. Bisher waren kostenlose Anonymisierungsdienste im Internet eine Möglichkeit für Bürger, sich unerkannt im Internet zu bewegen ohne Datenspuren zu hinterlassen, was in Zeiten globaler Datensammlungen durch privatwirtschaftliche Unternehmen durchaus im Sinne des Datenschutzes, aber auch verfassungsrechtlich durch das Grundrecht auf informationelle Selbstbestimmung garantiert ist.

Ebenso konnten diese Dienste bisher genutzt werden, wenn eine unbeobachtete Kommunikation notwendig erschien oder die durch einen Nutzer abgerufenen Inhalte, etwa von Aids-Beratungsstellen keine Rückschlüsse auf den Nutzer selbst zulassen sollten. Letztlich dienen freie Anonymierungsdienste wie TOR[52] Bürgern in Ländern, in denen es keine oder nur eingeschränkte Presse- und Meinungsfreiheit gibt, in denen Informationen der Zensur unterliegen wie etwa der VR China als eine Möglichkeit, unbeobachtet Inhalte aus dem Internet abzurufen, die durch ihre Regierungen zensiert werden.

Mit der Einbeziehung dieser Dienste wird eine anonyme Kommunikation, das heißt von Überwachung freie Kommunikation, wie sie bisher Ausdruck einer freiheitlichen Gesellschaftsauffassung war, faktisch abgeschafft. Was dies etwa für den investigativen Journalismus in Deutschland bedeutet, braucht keine Erklärung: Die geplante Gesetzgebung zur Vorratsdatenspeicherung beschädigt den „*[...] durch das Zeugnisverweigerungsrecht bezweckten Schutz der Informanten und [die] [...] von staatlichen Eingriffen ungestörten Redaktionsarbeit nachhaltig [...]*“[53].

Der Referentenentwurf orientiert sich bei den die

50 Bundesministeriums der Justiz: Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (RB 3 zu: 4104/11 - R5 884/2006), S.146

51 Im Grundgesetz kommt dieser zentrale Pfeiler des Strafrechts in Art 20 GG zum Ausdruck. Die Europäische Menschenrechtskonvention beinhaltet ihn ausdrücklich in Art. 6: „ [...] Jede Person, die einer Straftat angeklagt ist, gilt bis zum gesetzlichen Beweis ihrer Schuld als unschuldig.“

52 The onion routing: http://tor.eff.org

53 Gemeinsame Stellungnahme von ARD, BDZV, DJV, Deutscher Presserat, VDZ, Ver.di, VPRT und ZDF zum Referenten-Entwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, 19.01.2007, S.3 http://www.presserat.de/fileadmin/download/Stellungnahme_Telekommunikationsueberwachung.pdf abgerufen 10.04.2007

Vorratsdatenspeicherung umfassenden Daten an der EU-Richtlinie, geht aber mit den geforderten personenbezogenen Daten[54] über die Richtlinie hinaus.

Auch im Referentenentwurf werden die Anbieter von öffentlich zugänglichen Kommunikationsnetzen zur Speicherung der so genannten „Verkehrsdaten“ verpflichtet. Diese schließen bei Telefondiensten die Rufnummern der Kommunikationsteilnehmer, die Dauer und den Zeitpunkt des Vorganges, die Dienstart, sowie bei Mobiltelefonie – Mobilgerätekennung, Mobilkartenkennung und Standortdaten ein. Bei Kommunikationsvorgängen unter Nutzung des Internets sollen e-mail Adresssen, Anschlußkennung, Dienstart, zugewiesene IP-Nummer, Dauer und Zeitpunkt der Nutzung gespeichert werden.

Personenbezogene Daten[55] wie Anschrift, Name und Geburtsdatum des Anschlußinhabers sollen immer dann gespeichert werden, wenn der Anbieter „Rufnummern vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern bereitstellt“.

Eine weitere Verschärfung der europäischen Richtlinie kann konstatiert werden, wenn man die durch den Entwurf formulierten Straftatbestände betrachtet, die neu in den Straftatenkatalog der Strafprozessordnung aufgenommen werden. So werden mit dem neuen § 100g alle Straftaten erfasst, die „mittels Telekommunikation begangen werden“[56]. Hier wird nicht formuliert, welche Straftaten genau erfasst werden, ausschlaggebend ist allein die technische Infrastruktur, die bei Begehung der Straftat genutzt wurde. Bei dieser Verschärfung handelt es sich jedoch wahrscheinlich nicht um eine Interpretation der EU-Richtlinie selbst, vielmehr soll wohl der „Convention on Cybercrime“ entsprochen werden. Dennoch ist die durch das Justizministerium getroffene Formulierung viel zu unscharf, um hier den Willen einer Eingrenzung auf schwere Straftatbestände erkennen zu lassen, eine Überprüfung der Verhältnismäßigkeit einer aus der Formulierung folgenden Eingriffstiefe hat demnach wohl kaum stattgefunden.

Wie gezeigt wurde, handelt es sich bei dem Referentenentwurf nicht um eine spezifisch deutsche Interpretation der EU-Richtlinie zur Vorratsdatenspeicherung allein. Vielmehr werden mit ihm Abkommen und Entscheidungen, denen supranationale Akteurskonstellationen zugrunde liegen, „durch die Hintertür“ auf den deutschen Rechtsraum übertragen. So hält auch Jörg Tauss (MdB) eine Umsetzung der EU-Richtlinie für unumgänglich: „*[....] Wir haben diese Richtlinie nun einmal umzusetzen. Würden Sie deswegen nicht auch konstatieren, dass sich hier etwas an der Lage geändert hat? Wir müssen eine Richtlinie*

54 vgl. ebd. Änderung des Telekommunikationsgesetzes § 111 S. 37

55 Daten sind personenbezogen, wenn sie eindeutig einer bestimmten Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann. Im zweiten Fall spricht man auch von personenbeziehbaren Daten.

56 vgl. ebd. Änderungen der Strafprozessordnung §100g S. 22

umsetzen, ob sie uns gefällt oder nicht.“[57]

Welche Implikationen ergeben sich nun aus der europäischen Richtlinie und dem deutschen Referentenentwurf für Deutschland, das den Untersuchungsgegenstand dieser Arbeit darstellt? Ist der deutsche Gesetzgeber wirklich an eine Umsetzung gebunden, wie immer wieder von der Politik argumentiert wird oder lassen sich Gegenargumente finden? Wie steht es um die verfassungsrechtliche Vereinbarkeit des Referentenentwurfs und welche Folgen sind für die freiheitlich-demokratische Grundordnung bei Umsetzung des Entwurfes zu erwarten?

4.2 Umsetzungspflicht

Wie bereits beschrieben wurde aufgrund der schwierigen Interessenlagen der europäischen Nationalstaaten im Hinblick auf eine einheitliche Regelung für eine Vorratsdatenspeicherung auf EU-Ebene der Weg einer Richtlinie als Element der ersten Säule, dem Vertragswerk der Europäischen Gemeinschaft gewählt. So argumentieren Rat, Kommission und Europäisches Parlament[58], dass eine Notwendigkeit für die Angleichung von Speicherfristen und anderen, in den Nationalstaaten verschieden geregelten Verfahrensformen im Kommunikationssektor vorliegt, da andernfalls der gemeinsame Binnenmarkt behindert sei. Hieraus ergebe sich eine Handlungsgrundlage nach Art. 95 EG, der unter Anderem die Angleichung von Rechtsvorschriften zur Stärkung des gemeinsamen Binnenmarktes vorsieht.

Diese Ansicht ist stark umstritten. So vertreten einige Mitgliedsstaaten wie Irland und die Slowakei die Auffassung, die Europäische Gemeinschaft sei in diesem Fall nicht zuständig, da es primär nicht um die Angleichung von Rechtsnormen zur Schaffung eines besseren Binnenmarktverkehrs ginge, sondern vornehmlich um eine stärkere Zusammenarbeit im Bereich der Strafverfolgung, die in der dritten Säule – der Polizeiliche und justizielle Zusammenarbeit in Strafsachen - angesiedelt ist.

Auch der deutsche Bundestag hatte bis 2006 noch Zweifel[59] an der formellen Rechtmäßigkeit der Richtlinie: „*Der Deutsche Bundestag hat in seiner Stellungnahme vom Januar 2005 deutlich gemacht, dass er die Rechtsgrundlage für eine Regelung zur Vorratsdatenspeicherung in einem Rahmenbeschluss und damit in der „Dritten Säule“ (EUV) sieht: „Dass sich die nun geplante Maßnahme auf Artikel 95 EGV [...] stützt, begegnet Bedenken, [da] [...] die Richtlinie primär Strafverfolgungsinteressen verfolgt.*“[60]

57 Bettina Winsemann: "2006 – da sind wir völlig machtlos", bei Telepolis, 20.02.2006, http://www.heise.de/tp/r4/artikel/22/22085/1.html abgerufen 03.04.2007

58 vgl. RiL 2006/24/EG S.1f

59 vgl. Bundestags-Drucksache 16/545, 16/1622

60 vgl. Bundestags-Drucksache 16/545, S. 3 Abs. 13

Mittlerweile hat Irland Nichtigkeitsklage gegen die Richtlinie zur Vorratsdatenspeicherung vor dem Europäischen Gerichtshof (EuGH) eingereicht[61], die zwar noch nicht entschieden ist, deren Chancen auf Erfolg durch die Entscheidung des EuGH zur Fluggastdatenübermittlung an die USA aber gestiegen sind. Auch in diesem Fall wurde in Art. 95 EGV eine Handlungsgrundlage gesehen. Da Fluggesellschaften zur Erbringung ihrer Dienstleistungen Daten erheben und sich durch verschiedene nationale Regelungen diesbezüglich Nachteile für den gemeinsamen Binnenmarkt ergeben können, sei Regelungskompetenz durch die „erste Säule" gegeben. Der Europäische Gerichtshof folgte dieser Argumentation nicht, vielmehr sei die Fluggastdatenübermittlung eine zusätzliche Datenverarbeitung, *„die nicht für die Erbringung einer Dienstleistung" erforderlich sei, sondern vielmehr „zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken" dient*[62].

Mit diesem Urteil ist durch den EuGH ein Weg vorgezeichnet worden, der wohl auch beim Streitfall der Richtlinie zur Vorratsdatenspeicherung zu gehen sein wird, da zu erwarten ist, dass auch in diesem Fall das fehlen einer Rechtsgrundlage durch das Gericht festgestellt werden wird. Somit bliebe den Akteuren auf europäischer Ebene nur noch der steinige Weg über einen Rahmenbeschluss oder aber die Änderung der primärrechtlichen Rechtsgrundlagen.

Für den deutschen Gesetzgeber sollten die bisherigen Bedenken von Seiten des Bundestages, der Wirtschaft, von Bürgerrechtlern und der Wissenschaft eigentlich schon genug Anlass zum Umdenken in dieser Angelegenheit geführt haben. Das EuGH-Urteil zeigt seit Mitte 2006 deutlich auf, dass die Bedenken begründet und die Richtlinie auf wackligen Beinen steht, wenn sie nicht gar aufgrund formeller Fehler und Missachtung materieller Rechtsnormen rechtswidrig ist. Somit ist auch zweifelhaft, ob Deutschland zur Umsetzung der Richtlinie verpflichtet ist[63], solange die Nichtigkeitsklage Irlands nicht entschieden und die Vereinbarkeit mit den Grundsätzen der Europäischen Menschenrechtskonvention (EMRK) nicht geklärt[64] ist. Die zu erwartenden Kosten[65] einer Umsetzung der Richtlinie stehen in keinem Verhältnis zur derzeitigen Unsicherheit über die Rechtmäßigkeit der Richtlinie.

---

61 Az. C-301/06

62 vgl. EuGH, Urteil vom 30.05.2006, Rs. C-317/04 und C-318/04 Abs. 57

63 vgl. hierzu Stellungnahme des Arbeitskreises Vorratsdatenspeicherung vom 07.01.2007 zum Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwa chung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, S.3, http://www.vorratsdatenspeicherung.de/images/stellungnahme_vorratsdatenspeicherung.pdf abgerufenen 05.04.2007

64 Betroffen sind hier unter anderem Art. 8: Recht auf Achtung des Privat- und Familienlebens; Art. 10: Freiheit der Meinungsäußerung; Art. 6: Recht auf ein faires Verfahren EMRK.

65 Die Schätzungen für die Kosten einer 6-monatigen Datenspeicherung gehen weit auseinander. Der BITKOM-Verband geht von hohen bis mittleren zweistelligen Millionenbeträgen aus. vgl. BITKOM Pressemitteilung von 15.03.2005: Datenspeicherpflichten gefährden Wachstum im Hightech-Sektor, http://www.bitkom.org/files/documents/PI_BITKOM_und_BDI_Vorratsdatenspeicherung_15_03_2005.pdf sowie Heise: Vorratsdatenspeicherung kommt die TK-Branche teuer zu stehen, http://www.heise.de/newsticker/meldung/87932/from/rss09 abgerufen am 05.04.2007

Dass die politischen Verantwortungsträger derzeit eher noch an einer weiteren Verschärfung etwa der präventiven Ermittlungskompetenzen von BKA und BND interessiert sind und ein Überdenken geplanter und bereits umgesetzter Gesetzte nicht in Frage zu kommen scheint, zeigt die Entwicklung auf, die im Zentrum dieser Arbeit steht – der präventiven Wende in der Innen- und Sicherheitspolitik: vom repressiven Rechtsstaat in die präventive Kontrollgesellschaft[66].

Welcher Natur diese Wende hin zu einer präventiven Strafverfolgung entspricht, kann aus dem bisher gesagten bereits erahnt werden, welche Folgen durch die neue Handlungslogik mit Blick auf den freiheitlich-demokratischen Rechtsstaat zu erwarten sind, wird im folgenden anhand der verfassungsrechtlichen Problematik erörtert werden.

4.3 Grundrechtsschutz und Vorratsdatenhaltung

Die geplante Vorratsdatenspeicherung sieht vor, die bei Kommunikationsvorgängen bei den Anbietern öffentlicher Kommunikationsnetze entstehenden Verkehrsdaten aller rund 80 Mio. deutschen Bürger für sechs Monate auf Vorrat speichern zu lassen. Somit sind alle Teilnehmer des gesellschaftlichen Lebens unmittelbar von der Maßnahme betroffen, was ein Hinweis auf die Eingriffstiefe, einem Faktor zur Bewertung der Verhältnismäßigkeit von staatlichen Eingriffen, liefert. Da sich die zu speichernden Daten nicht im Einflussbereich der betroffenen Personen befinden, die Maßnahme heimlich und verdachtsunabhängig stattfindet, ist von einer starken Eingriffstiefe in die Persönlichkeitsrechte, vor allem das Recht auf informationelle Selbstbestimmung[67] und das Fernmeldegeheimnis (Art. 10 GG) auszugehen.

Weiterhin werden auch die Anbieter von Kommunikationsdiensten in ihren Grundrechten beschnitten, da eine Speicherung von Kommunikationsdaten über das betriebswirtschaftlich nötige Maß und zu anderen Zwecken als von den Anbietern benötigt, eine Inanspruchnahme Privater für öffentliche Aufgaben bedeutet, was wiederum eine Einschränkung der Berufsfreiheit und des Rechts am Eigentum bedeuten kann.

Einschnitte in Grund- und Bürgerrechte bedürfen der Begründung durch den Gesetzgeber[68] und müssen dem Grundsatz der Verhältnismäßigkeit gerecht werden. Eine staatliche Maßnahme ist dann verhältnismäßig, wenn sie einen bestimmten Zweck nennt, der erfüllt werden soll. Die zur Erfüllung dieses Zwecks genutzten Mittel müssen geeignet, erforderlich sowie angemessen sein.

66 vgl. Heise „Schäubles lange Liste für weitere Ermittlungsbefugnisse “, http://www.heise.de/newsticker/meldung/87714/ abgerufenen 10.04.2007

67 Das informationelle Selbstbestimmungsrecht ist eine Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) und wurde vom Bundesverfassungsgericht im so genannten Volkszählungsurteil 1983 als Grundrecht anerkannt.

68 Als verfassungsrechtliches Gebot ist das Verhältnismäßigkeitsprinzip gem. Art. 1 Abs. 3, Art. 20 Abs. 3 GG für die gesamte Staatsgewalt unmittelbar verbindlich.

Im Falle der geplanten Vorratsdatenspeicherung ist davon auszugehen, dass der Gesetzgeber von der Natur der Sache her diesen Anforderungen schon nicht gerecht werden kann. Eine verdachtsunabhängige Speicherung von Kommunikationsdaten auf Vorrat zur Verhinderung terroristischer Bestrebungen und schwerer Straftaten ist keine hinreichende Zweckbestimmung, wie sie vom Grundgesetz gefordert wird. Vielmehr ist hierdurch die Umkehr eines alten rechtsstaatlichen Prinzips gegeben, der Unschuldsvermutung. Nach ihm kann eine Schuld erst dann anerkennt und gesühnt werden, wenn sie zweifelsfrei belegt ist. Mit der Vorratsdatenspeicherung wird aber jedermann unter Verdacht gestellt, jetzt oder in Zukunft eine zumindest erhebliche Straftat zu begehen. Zur allgemeinen Gefahrenabwehr wird hier also ein eine Überwachungsmaßnahme eingesetzt, die jeden mündigen Bürger betrifft, egal ob es Anzeichen für ein „fehlerhaftes“ Verhalten gibt oder nicht. Das ist mit rechtsstaatlichen Grundsätzen nicht zu vereinbaren.

Eine Vorratsdatenspeicherung ist auch nicht geeignet, um Straftaten erheblicher schwere zu verhindern, da die Maßnahme bei ausreichendem technischem Wissen durch einen potentiellen Straftäter einfach umgangen werden kann[69]. Zwar kann wohl von einigen Erfolgen bei der Ermittlung von bereits begangenen Straftaten ausgegangen werden, eine präventive Wirkung wird sich hier aber wohl – zumindest bei schweren Straftaten - nicht entfalten können.[70] Eine solche, auf die Allgemeinheit ausgerichtete Maßnahme wird auch nicht zur Förderung des in Aussicht gestellten Zwecks führen. Vielmehr wird der Personenkreis, der Ziel der Maßnahme ist, auf sichere Kommunikationswege ausweichen. Der breiten Masse der Betroffenen erschließt sich diese Möglichkeit jedoch nicht, was zu wachsendem Misstrauen gegenüber staatlichen Institutionen führen und eine sozio-politische Stigmatisierung von Betroffenen[71] fördern kann.

Die Erforderlichkeit der Vorratsdatenspeicherung als Mittel der Strafverfolgung und präventiven Gefahrenabwehr wird zwar immer wieder durch die politischen Verantwortungsträger beteuert, jedoch nie in Zahlen und Fakten belegt. So wird argumentiert, dass Daten, die zur Ermittlung von Straftätern nötig wären, oft von den Dienstanbietern bereits gelöscht wurden, bevor eine Behörde sie auswerten konnte. Vergessen wird hierbei - offensichtlich beabsichtigt – dass es bereits Möglichkeiten gibt, Daten „auf Zuruf“ von Seiten der Anbieter einfrieren zu lassen (§§ 100a, 100b, 100g sowie 100h StPO). Auch wurde durch

69 vgl. hierzu Marc Störing: „LG Konstanz: Zugriff auf Anonymisierungsserver“, in: MMR 2007 Heft 3 S. 194ff; Kai Raven: „Sicher und anonym im Internet mit Proxys“, http://hp.kairaven.de/bigb/asurf.html abgerufen 10.04.2007; sowie Hannes Federrath: „Das AN.ON-System: Starke Anonymität und Unbeobachtbarkeit im Internet“

70 Es handelt sich bei den erhobenen Daten schließlich um keine Echtzeit-Mitschnitte des Datenverkehrs, sondern um einen historischen Rückblick auf Kommunikationsvorgänge. Somit lassen sich Kommunikationsvorgänge rekonstruieren, aber nicht vorwegnehmen.

71 Es sei hier an die Debatten und Medienkampagnen zu „Terror-Zellen“ an Universitäten und „islamistischen Schläfern“ allerorten einige Zeit nach den Anschlägen des 11. Septembers erinnert, die zu einiger gesellschaftlicher Distanz zu „islamistisch wirkenden“ Personen in der Öffentlichkeit geführt haben dürften. Auch das Mittel der Rasterfahndung zeitigte keinerlei Erfolge, führte aber zur Stigmatisierung einiger Bevölkerungsgruppen anhand scheinbar willkürlich ethischer Fahndungsraster.

die nicht unumstrittene Telekommunikationsüberwachungsverordnung (TKÜV) bereits ein weiteres Mittel geschaffen, dass das Protokollieren auch von Inhaltsdaten in Echtzeit möglich macht. Es ist also mitnichten richtig, dass es keine Handhabe für die neuen technischen Herausforderungen der Ermittlungsarbeit gäbe.

Eine alle Bürger betreffende Vorratsdatenspeicherung kann auch nicht als angemessen angesehen werden. So ist bei Eingrenzung der behördlichen Zugriffsbefugnisse auf schwere und erhebliche Straftaten davon auszugehen, das die Strafverfolgungsbehörden nur einen Bruchteil (circa 0.0004%[72]) der anfallenden Daten überhaupt jemals abfragen würden, von der Speicherung aber 99% unschuldige, redliche Bürger betroffen sein werden.

Somit kann derzeit angenommen werden, dass eine Vorratsdatenspeicherung den verfassungsmäßigen Anforderungen nicht gerecht werden kann, da sie weder einer bereichsspezifischen noch präzisen Zweckbindung unterliegt, nicht als geeignet, angemessen oder erforderlich im Sinne der Rechtssprechung des Bundesverfassungsgerichts angesehen werden kann[73].

4.4 Zwischenfazit

Wie gezeigt wurde, ist der Gesetzgeber gerade dabei, auf Bundesebene eine Zeitenwende in der Innen- und Sicherheitspolitik einzuleiten. Es handelt sich hierbei um eine Wende, die nicht mehr alten Rechtsstaatsprinzipien zu folgen scheint, vielmehr sollen präventive Kontrollmechanismen normiert werden, die dem Ideal einer „sicheren Gesellschaft“, wie sie in Zeiten wachsender Unsicherheiten im Interesse von politischen und sozialen Eliten zu sein scheinen, zuarbeiten.

Es handelt sich hierbei um eine mit der Einschränkung von Grund- und Bürgerrechten erkaufte Sicherheit, deren institutionelle und normative Pfeiler in den letzten Jahren zunehmend sichtbar werden. Der Gesetzgeber gibt sich in dieser Situation gegenüber seinen Bürgern als hilflos aus: Es werden Umsetzungszwänge aufgrund von internationalen Abkommen formuliert, die Notwendigkeit von neuen Mitteln der „Strafverfolgung“ stilisiert, neue Gefahrensituationen heraufbeschworen[74] sowie alte Feindbilder[75] neu bewertet, um dem verunsicherten Souverän alle nötigen Mittel zu entlocken und einen

72 Bianca Uhe, Jens Herrmann: *Überwachung im Internet – Speicherung personenbezogener Daten auf Vorrat durch Internet Service Provider.* Diplomarbeit. Berlin 2003, S. 161 http://ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf abgerufen 11.04.2006

73 So auch RA Leutheusser-Schnarrenberger (MdB): Vorratsdatenspeicherung - Ein vorprogrammierter Verfassungskonflikt, in Zeitschrift für Rechtspolitik 2007 Heft 1, S.9ff

74 So warnte etwa Innenminister Wolfgang Schäuble bei Spiegel-Online vor Terroranschlägen mit „Schmutzigen Bomben“: http://www.spiegel.de/politik/deutschland/0,1518,397686,00.html abgerufenen 04.04.2007

75 So etwa die Übertragung gesellschaftlicher Probleme auf das Internet, das oft als das „Medium des Bösen“ angesehen wird, in dem es nur so von politischen Extremisten, Kinderpornographen, Bombenbauern und ähnlichen subversiven Elementen wimmelt. Vergleicht man, wie in Kapitel 2 dieser Arbeit, die wirkliche Dimension des Internets als Plattform für Straftaten, so stellt sich heraus, dass das Internet eher die gesellschaftliche Realität widerspiegelt.

neuen, absoluten Leviathan zu schaffen.

Bisher wurde stets angenommen, Grund- und Bürgerrechte seien Rechte des Souveräns *vor* dem Staat, die diesen daran hindern, zu tief und willkürlich in das selbst bestimmte Leben seiner Bürger einzugreifen. Meinungsfreiheit, informationelle Selbstbestimmung, Pressefreiheit, das Recht auf einen gerechten Prozess – das sind einige der Rechte, die bisher zum Wohle einer freiheitlich-demokratischen Gesellschaft als unantastbar galten. Die neue innenpolitische Denkart sieht sich durch diese Rechte in der Handlungsfähigkeit bei der Durchsetzung von Sicherheit eingeschränkt und ist seit Jahren an der Umdeutung der diesen Grundrechten zugrunde liegenden Vorstellungen beteiligt. So wird durch die politischen Verantwortungsträger Sicherheit als höchstes Rechtsgut definiert, ohne das eine Ausübung von Grundrechten wie der Pressefreiheit gar nicht möglich wäre. Somit wird ein abstrakter Sicherheitsbegriff in öffentlichen Diskursen als fundamentale Staatsaufgabe begriffen und über die zu sichernden Grundrechte gestellt.

Die perfide Logik dieser seit einigen Jahren zu beobachtenden Bestrebungen endet dann in Gesetzesentwürfen wie dem Referentenentwurf zur Vorratsdatenspeicherung, dessen fundamentale formale und materielle Rechtswidrigkeit bereits beschrieben wurde.

Die in dieser Arbeit anhand der geplanten Vorratsdatenspeicherung konstatierte präventive Wende kann als ein Puzzleteil angesehen werden, das die Entwicklung von einem liberalen Rechtsstaat hin zu einem digitalen Leviathan kennzeichnet: Es „*[...] lassen sich Anzeichen eines politischen Gestaltungswillens erkennen, indem Bedrohungsszenarien aufgebaut und politisch instrumentalisiert werden. [...]*“[76]. Um diese Entwicklung weiter zu verdeutlichen, folgt nun eine überblicksartige Zusammenschau und kritische Würdigung verschiedener weiterer gesetzgeberischer Weichenstellungen im Bereich der Innenpolitik auf Bundes- und Länderebene.

5 Der digitale Leviathan – ein Hochseilakt des Rechtssaates

5.1 Sicherheitspolitik 9/11

Nach den terroristischen Anschlägen in Amerika wurden zahlreiche Gesetzesinitiativen - ohne einer tiefen öffentlichen Diskussion Raum zu geben - gestartet, die den Beginn der präventiven Wende[77]

76 Stephan Heinrich: Auf dem Weg in einen Überwachungsstaat? Informationssicherheit und Kontrolle in offenen Kommunikationsnetzen, Marburg: Tectum-Verl., 2004 S. 113

77 vgl. hierzu Dirk Heckmann: Sicherheitsarchitektur im bedrohten Rechtsstaat – Neue Polizeibefugnisse zwischen gestalterischer Freiheit und grundrechtlicher Statik, in: Sicherheit statt Freiheit? : staatliche Handlungsspielräume in extremen Gefährdungslagen, Ulrich Blaschke (Hrsg.), Berlin : Duncker & Humblot, 2005, S. 12f

kennzeichneten. So wurden die Schranken für die Durchführung von Rasterfahndungen gelockert, die Zusammenarbeit zwischen Geheimdiensten und Ermittlunsbehörden erleichtert, die Erkennungsdienstliche Behandlung der Bevölkerung durch Aufnahme von biometrischen Daten in Pässe und Ausweise beschlossen, die Kontrolle von Ausländern ausgeweitet sowie die Möglichkeiten der geheimen Ermittlungsarbeit erweitert[78].

Ein Beweis über die Wirksamkeit all dieser Maßnahmen konnte bisher nicht erbracht werden, vielmehr ist das Gegenteil der Fall: Die bundesweiten Rasterfahndungen im Gefolge des Terroranschlages des 11. September konnten keinerlei verwertbare Ergebnisse zeitigen, der Einschnitt in die Rechte der betroffenen Bürger sind dagegen überaus offenkundig und die Anfälligkeit dieses Mittels der Strafverfolgung für Missbrauch ebenfalls gut dokumentiert[79].

Eines haben all die Maßnahmenkataloge – ob Anti-Terror-Paket I, oder Schily-Katalog II, TKÜV oder großer Lauschangriff - gemein, sie sollen es den Strafverfolgungsbehörden und Geheimdiensten nach Möglichkeit erlauben, präventiv tätig zu werden und gleichzeitig weit reichende Kontrollstrukturen schaffen, die ein Eingreifen in das Leben der Bürger jederzeit technisch und rechtlich möglich machen[80]. So wurden mit der Einführung der biometrischen Daten auf Ausweisdokumenten erst die technischen Möglichkeiten geschaffen, die nun zu Überlegungen führen, eine Vernetzung und Zentralisierung dieser Daten in Datenbanken bei den Einwohnermeldeämtern durchzuführen.

5.2 Digitale „Revolution“ - Der Datenbürger

Die technische Revolution hat Möglichkeiten zur Kontrolle der Bürger geschaffen, die bisher nicht denkbar waren und die nun im Zentrum der in dieser Arbeit konstatierten präventiven Wende zu stehen scheinen. In der digitalen Welt ist ein Verzicht auf moderne Kommunikationsmedien dem Einzelnen nicht mehr möglich ohne Gefahr zu laufen, gesellschaftlich ausgegrenzt zu werden. Mit Nutzung dieser Medien wird eine Protokollierung seines Verhaltens, seiner Vorlieben, seiner sozialen Kontakte, seiner Geschäftsbeziehungen – kurz all seiner individuellen und gesellschaftsbezogenen Regungen - in maschinenlesbarer, das heißt digitaler Form möglich.

Welche Begehrlichkeiten die neuen technischen Möglichkeiten in der

78 vgl. hierzu Bürgerrechte & Polizei/CILIP 70 (3/2001): Terrorismusbekämpfung - alte und neue Irrwege

79 Zur Bewertung der Wirksamkeit und den Mängeln des Verfahrens der Rasterfahndung am Beispiel Berlin vergl. Berliner Beauftragten für Datenschutz und Informationsfreiheit: „Sonderbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 10.12.2002“, http://www.datenschutz-berlin.de/infomat/sonderbericht/rasterfahndung.pdf abgerufenen 10.04.2007

80 Vergleiche hierzu die zahlreichen Eingaben von Bürgerrechtsorganisationen wie der Humanistisches Union, Stop 1984, Arbeitskreis Vorratsdatenspeicherung,FoeBUD e.V. zu aktuellen und zurückliegenden Gesetzgebungsverfahren.

Politik wecken, kann aktuell gut beobachtet werden, wenn man die aktuellen Diskussionen um die neueren Planungen des derzeitigen Innenministers Wolfgang Schäuble rund um Online-Durchsuchung, Erweiterung präventiver Ermittlungskompetenzen und Biometriedatenbanken verfolgt[81]. Die fortschreitende Implementierung[82] der politisch gewünschten Kontrollmechanismen[83] führt geradewegs in eine Kontrollgesellschaft, in der die traditionellen Grundrechte nur noch als Fassade angesehen werden können. Anders ist die Forderung Schäubles[84] notfalls eine Grundgesetzänderung herbeiführen zu wollen, um Online-Durchsuchungen möglich zu machen wohl nicht zu verstehen.

Die grundrechtliche Entgrenzung des sicherheitspolitischen Diskurses ist nicht auf den Bund beschränkt. Wie bereits bei der Vorratsdatenspeicherung gezeigt wurde, nehmen auch die Bundesländer ihre Verantwortung im Sinne der präventiven Wende seit Jahren in vollem Umfang war.

5.3 Landespolitische Einzelinitiativen

Der auf Bundesebene zu beobachtende neue innenpolitischen Maxime sind auf Ebene der Länder die zahlreichen Novellierungen der Polizeigesetze gleichzusetzten.

So wurden in Berlin (2003), Niedersachsen (2003), Hessen (2004), Brandenburg (2006) sowie Kiel (2007) neue Polizeigesetze erlassen, deren Stoßrichtung mit jeweils verschiedener Reichweite und Fokussierung jedoch immer auf die Erweiterungen präventiver Kompetenzen und Zugriffsmöglichkeiten zielt.

Im Falle des neuen Berliner Polizeigesetzes (ASOG[85]) wurde von Seiten der Bürgerrechtler vor allem die Ausweitung der Videoüberwachung kritisiert: „Das Netz privater und staatlicher Videoüberwachung in Berlin wird durch die zusätzliche polizeiliche Erfassung sogenannter "gefährdeter Objekte" noch engmaschiger.“[86]

Das niedersächsische Polizeigesetz sieht eine vereinfachte Telefonüberwachung auch ohne konkreten Verdacht vor, der vorsorgliche Polizeigewahrsam wird vereinfacht[87], wohingegen in

81 vgl. hierzu u.a. Christian Raths: Fahnden mit dem Passfoto in: taz vom 12.4.2007, S. 6

82 Als aktuelles Beispiel sei hier die Anti-Terror-Datei angeführt, die bisher dezentrale Datenbanken zum Zwecke der Gefahrenabwehr zusammenfassen soll, darunter fallen auch Daten wie die Fingerabdrücke von Asylantragstellern. vgl. hierzu Heise: Von der Anti-Terror-Gesetzgebung zur Anti-Terror-Datei, http://www.heise.de/ct/hintergrund/meldung/85995 abgerufenen am 10.04.2007

83 Gemeint sind hier einerseits die Ausweitung der präventien Ermittlungskompetenzen auf Landes- und Bundesebene sowie das Errichtung der hierfür notwendigen Datenbestände, wie etwa Kommunikationsverkehrsdaten, biometrischen Daten, statischischen Daten, sowie Datenbestände zu sozialen, wirtschaftlichen, religiösen und politischen Einstellungen der Bürger.

84 vgl. Heise: Kritik von Datenschützern ist für Bundesinnenminister Schäuble "naiv", http://www.heise.de/newsticker/meldung/87894 abgerufenen 10.04.2007

85 Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin

86 vgl. Stellungnahme der Humanistischischen Union Berlin zum neuen ASOG: Einführung polizeilicher Videoüberwachung: Bürgerrechtler sehen trotz Nachbesserung Gefahr, http://berlin.humanistische-union.de/aktuelles/andere_beitraege/andere_detail/back/andere-beitraege/article/einfuehrung-polizeilicher-videoueberwachung-buergerrechtler-sehen-trotz-nachbesserung-gefahr/ abgerufenen am 10.04.2007

87 vgl. Heise: Niedersachsen bekommt verschärftes Polizeigesetz, http://www.heise.de/newsticker/meldung/42842 abgerufenen am

Hessen die automatische Erfassung von Autokennzeichen zur Fahndung, erweiterte Befugnisse zur Telefon- und Videoüberwachung, zur Ermittlung von Standortdaten von Mobilfunknutzern sowie die Legalisierung neuer Überwachungsmethoden (IMSI-Catcher, Erfassung von DNA- und biometrischen Daten auch bei Minderjährigen) vorgesehen[88] sind. Ähnliche Anpassungen wurden auch in Brandenburg und Kiel vorgenommen[89], auch wenn die hier verabschiedeten Gesetze in Sachen Prävention und Kontrolle analog zur bundespolitischen Debatte noch um einiges weitreichender sind, als etwa die vergeichsweise sanfte Ausgestaltung der nun schon in die Jahre gekommenen berliner Reform des .

Die Verschiebung der polizeilichen Zuständigkeit hin zur Generalprävention wird mit den angeführten Änderungen im Polizeirecht deutlich, die in Ballungszentren ergänzt wird durch die zunehmende Privatisierung öffentlicher Plätze und damit einher gehend der Übertragung von hoheitlichen Aufgaben im Sicherheitsbereich auf private Sicherheitsdienstleister[90].

Insgesamt kann davon ausgegangen werden, dass die präventive Wende, wie sie hier dargestellt wurde auf allen politische Ebenen vorzufinden ist und die neue sicherheitspolitische Dogmatik, in der ein diffuser Sicherheitsbegriff über den Gedanken der Grundrechte als Rechte *vor* dem Staat gestellt wird, alle politischen Diskurse bestimmt. Es ist derzeit nicht abzusehen, wann die Gegenseite die argumentative Übermacht zu Gunsten der Grund- und Bürgerrechte wieder erlangen wird und ob dies mit Hinblick auf die bereits geschaffen Tatsachen in einem solchen Fall überhaupt noch eine Verbesserung der Grundrechtspositionen des Einzelnen bewirken kann.

6 Zusammenfassung und Ausblick

Wie gezeigt werden konnte erlebt die Innen- und Sicherheitspolitik gerade eine präventive Wende, deren Handlungslogik sich scheinbar ausschließlich an einem diffusen Sicherheitsbegriff festzumachen scheint. Dieser Logik gegenüber können traditionelle Vorstellungen der Grundrechtssicherung als Abwehrrechte vor der Allmacht des Staates kaum noch Wirkung entfalten: Es findet „*[...] unter dem Stickwort des Präventionsstaates ein fundamentaler Paradigmenwechsel statt. Zunehmend wird Sicherheit und Freiheit als Schutz durch den Staat verstanden. [...]*“[91]

10.04.2007

88 vgl. Heise: Hessen dehnt Polizeibefugnisse deutlich aus, http://www.heise.de/newsticker/meldung/54298 abgerufenen am 10.04.2007

89 vgl. Heise: Kieler Landtag winkt verschärftes Polizeigesetz durch, http://www.heise.de/newsticker/meldung/85739 abgerufen am 10.04.2007 sowie Heise: Brandenburg erhält deutlich verschärftes Polizeigesetz, http://www.heise.de/newsticker/meldung/82598 abgerufenen am 10.04.2007

90 Die Behandlung dieser Thematik würde den Rahmen dieser Arbeit deutlich sprengen, daher sei hier auf die Dissertation von Benno Kirsch: Private Sicherheitsdienste im öffentlichen Raum : Formen und Folgen der Zusammenarbeit mit der Polizei in Berlin und Frankfurt am Main, Wiesbaden : Westdt. Verl., 2003 verwiesen.

91 Kyrill-A. Schwarz: Die Dogmatik der Grundrechte – Schutz und Abwehr im freiheitssichernden Staat, in: Sicherheit statt Freiheit? : staatliche Handlungsspielräume in extremen Gefährdungslagen, Ulrich Blaschke (Hrsg.), Berlin : Duncker & Humblot, 2005, S.31

Notfalls sollen hinderliche Grundrechtspositionen, wie sie etwa im Grundgesetz oder in der einschlägige Rechtssprechung des Bundesverfassungsgerichts als Begrenzung der staatlichen Einflusszonen formuliert wurden, zur Legalisierung neuer Gesetzgebungen dem sicherheitspolitischen Bedürfnissen angepasst werden.

Die neuen technischen Entwicklungen und die voranschreitende Globalisierung haben auch den Gesetzgeber vor neue Herausforderungen gestellt, so etwa der internationale Terrorismus, die weltweit agierenden Wirtschaftskriminalität, die neuen Kommunikationswege und Formen der gesellschaftlichen Interaktion über Kontinente hinweg. Mit der Globalisierung und der hiermit verbundenen wirtschaftlichen, sozialen und gesellschaftspolitischen Veränderungen wächst in den Wettbewerbsgesellschaften – oft auch als Risikogesellschaft betitelt – die allgemeine Unsicherheit, sei sie persönlicher, politischer, wirtschaftlicher oder ökologischer Natur.

Die neue geopolitische Situation, die Nationalstaaten an die Grenzen ihrer Handlungsfähigkeit führt, verbunden mit der steigenden Unsicherheit in der Bevölkerung haben zu einem Paradigmenwechsel in der Sicherheitspolitik geführt, der ausgehend vom Konzept der Risikogesellschaft die Grenzen zwischen geforderter Sicherheit und gewünschter Freiheit neu definiert. So wird der Grundrechtsgedanke, der die staatliche Kontrolle zugunsten einer freiheitlichen Gesellschaft eindämmen soll, mittlerweile unter den Vorbehalt von diffusen Sicherheitsinteressen gestellt. Freiheit kann nur über Sicherheit gewährleistet werden, so das Kredo des neuen sicherheitspolitischen Paradigmas, das in dieser Arbeit auf den verschiedenen politischen Ebenen nachgewiesen wurde.

Es konnte gezeigt werden, dass die präventive Wende auf internationaler, europäischer, nationaler und föderaler Ebene bereits weit fortgeschritten und durch internationale Abkommen, europäische Rechtssetzungen, nationale Gesetzgebungsverfahren sowie Reformen der föderalen Polizeigesetze normativ implementiert wurde.

Die zunehmende Digitalisierung des gesellschaftlichen Lebens und neue technologischen Entwicklungen wie etwa die der Biometrie, die RFID-Chiptechnologie oder neuen Methoden der Videoanalyse führen zu schier unstillbaren Begehrlichkeiten von Seiten der politischen Verantwortungsträger, aber auch der Privatwirtschaft. Diese laufen Gefahr, das traditionelle freiheitlich-demokratische Grundverständnis, wie es die westlichen Demokratien charakterisiert und auf dessen grundrechtlichen Pfeilern höhere Rechtsgüter wie die der allgemeinen Menschenrechte ruhen, zu unterlaufen und zu unterhöhlen.

Die immer lückenloseren Datenbestände und unbegrenzten Analysemöglichkeiten dieser Daten führen vielleicht nicht in einen

Orwellschen Überwachungsstaat – dafür fehlt es am polischen Totalitarismus - wohl aber zu einer kontrollierten Gesellschaft, in der sich nur Individuen „frei“ entfalten können, die den herrschenden Normen entsprechen.

Es darf mit Spannung erwartet werden, wie lange die beschriebene Wende in der Sicherheitspolitik noch fortgeschrieben werden kann, wie lange die Bürger noch bereit sein werden, auf Grundrechte zugunsten eines diffusen Sicherheitsbegriffes zu verzichten. Die steigende mediale Aufmerksamkeit schürt zumindest die Hoffnung, das die Grenzen des politisch Durchsetzbaren langsam erreicht sind.

7 Literatur

Alvaro Alexander Nuno: Bericht zur Vorratsdatenspeicherung (A6-0174/2005), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0174+0+DOC+PDF+V0//DE

Arbeitskreises Vorratsdatenspeicherung: Stellungnahme vom 07.01.2007 zum Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwa chung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, http://www.vorratsdatenspeicherung.de/images/stellungnahme_vorratsdatenspeicherung.pdf

ARD/ZDF-Online-Studie 2006 zur Internetnutzung, http://www.ard-werbung.de/showfile.phtml/eimeren.pdf?foid=17746

ARD, BDZV, DJV, Deutscher Presserat, VDZ, Ver.di, VPRT und ZDF: Gemeinsame Stellungnahme zum Referenten-Entwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, 19.01.2007, http://www.presserat.de/fileadmin/download/Stellungnahme_Telekommunikationsueberwachung.pdf

Autengruber Christof: Vision und Realität Freirer Community Netze - Selbstorganisation in der Netzkultur, Magisterarbeit, Universität Salzburg, Januar 2007, http://www.dslnachpankow.de/cms/modules/PDlinks/visit.php?cid=15&lid=80

Beck Ulrich: Risikogesellschaft. Auf dem Weg in eine andere Moderne. Suhrkamp, Frankfurt a.M. 1986

BITKOM: Pressemitteilung von 15.03.2005: Datenspeicherpflichten gefährden Wachstum im Hightech-Sektor, http://www.bitkom.org/files/documents/PI_BITKOM_und_BDI_Vorratsdatenspeicherung_15_03_2005.pdf

Bundesministerium des Inneren (BMI): Polizeiliche Kriminalstatistik 2005 , http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2006/Polizeiliche__Kriminalstatistik__20054__de,templateId=raw,property=publicationFile.pdf/Polizeiliche_Kriminalstatistik_20054_de.pdf

Berliner Senatsverwaltung für Justiz: Pressemitteilung: Deutlicher Zuwachs an Internet-Straftaten: Bericht der Staatsanwaltschaft zur Entwicklung der Verfahrensdaten, Berlin 19.12.2005, http://www.berlin.de/sen/justiz/presse/archiv/20051219.26103.html

Blaschke Ulrich: Sicherheit statt Freiheit? : staatliche Handlungsspielräume in extremen Gefährdungslagen, Ulrich Blaschke (Hrsg.), Berlin : Duncker & Humblot, 2005

Bundesamt für Sicherheit in der Informationstechnik (BSI): Was ist Anonymität?, http://www.bsi.de/literat/anonym/wasist.htm

Bundesministerium für Justiz: Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 27.11.2006, http://www.vorratsdatenspeicherung.de/images/RefE-2006-11-27.pdf

Bundesministerium für Wirtschaft und Technologie: Informationen zur Telekommunikations-Überwachungsverordnung (TKÜV), http://www.bmwi.de/Navigation/Wirtschaft/telekommunikationundpost,did=6018.html

Bundesrats-Drucksachen 275/02, 14/9801 , 16/545 , 16/1622

„Convention on Cybercrime“ (Deutscher Volltext), Fassung vom 23.09.2001, http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm

Convention on Cybercrime CETS No.: 185 (Stand der Ratifikation),Stand 4.8.2006, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=8/4/2006&CL=ENG

Europäischen Parlament: Plenarprotokoll vom 7.Juni 2005 (P6_PV(2005)06-07)

Europäisches Parlament: Pressebericht zur Abstimmung - Plenarsitzung vom 14.12.2005 in Straßburg, http://www.europarl.de/presse/pressemitteilungen/quartal2005_4/PM_14122005_1

European Parliament plenary debate on Data Retention: Speech by Charles Clarke, UK Secretary of State for the Home Office, 13 December 2005 , http://www.eu2005.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1115146994906&a=KArticle&aid=1134649501007&date=2005-12-13

Europäische Kommission: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM/2005/0438)

Federrath Hannes: „Das AN.ON-System: Starke Anonymität und Unbeobachtbarkeit im Internet“ , in: Helmut Bäumler, Albert von Mutius (Hrsg.): Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Verlag Vieweg, 2003

Gercke Marco: Analyse des Umsetzungsbedarfs der Cybercrime Konvention: Umsetzung im Bereich des materiellen Strafrechts, in: MMR 2004 Heft 11, S. 728ff

Gercke Marco: Analyse des Umsetzungsbedarfs der Cybercrime Konvention: Umsetzung im Bereich des Strafverfahrensrechts, in: MMR 2004 Heft 12, S. 801ff

Glaeßner Gert-Joachim, Lorenz Astrid: Europäisierung der inneren Sicherheit : eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus, Gert-Joachim Glaeßner (Hrsg.), Wiesbaden: VS, Verlag für Sozialwissenschaft, 2005

Guardian The: Huge majority say civil liberty curbs a 'price worth paying' to fight terror, 24.Januar 2007: http://www.guardian.co.uk/terrorism/story/0,,1997283,00.html

Hanning August, Staatssekretär im Bundesministerium des Inneren in Tagesschau: Alltag Überwachung, http://213.200.64.229/tagesschau/mp3/misc/alltag-ueberwachung_komplett.mp4

Heinrich Stephan: Auf dem Weg in einen Überwachungsstaat? Informationssicherheit und Kontrolle in offenen Kommunikationsnetzen, Marburg: Tectum-Verlag, 2004

Heise News: 22C3: "Wir haben den Krieg verloren", http://www.heise.de/newsticker/meldung/67796

Heise News: Vorratsdatenspeicherung kommt die TK-Branche teuer zu stehen, http://www.heise.de/newsticker/meldung/87932/from/rss09

Heise News: Schäubles lange Liste für weitere Ermittlungsbefugnisse, http://www.heise.de/newsticker/meldung/87714/

Köpsell Stefan, Federrath Hannes, Hansen Marit: Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes, in: Datenschutz und Datensicherheit (DuD), 27/3 (2003),139

Rat der Europäischen Union: Entwurf für Schlussfolgerungen des Rates über IT-bezogene Maßnahmen im Hinblick auf die Ermittlung und Verfolgung organisierter Kriminalität, Brüssel 24.06.2002, http://register.consilium.eu.int/pdf/de/02/st10/10358d2.pdf

Raven Kai: Anleitungen und Einführungen, http://hp.kairaven.de/misc/anleitung.htm

Raven Kai: „Sicher und anonym im Internet mit Proxys“, http://hp.kairaven.de/bigb/asurf.html

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 , http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/oj/2006/l_105/l_10520060413de00540063.pdf

RA Leutheusser-Schnarrenberger (MdB): Vorratsdatenspeicherung - Ein vorprogrammierter Verfassungskonflikt, in Zeitschrift für Rechtspolitik 2007 Heft 1, S.9ff

Rost Martin: Zur gesellschaftlichen Funktion von Anonymität – Anonymität im soziologischen Kontext, in: Datenschutz und Datensicherheit (DuD), 27/3 (2003), 155

Spiegel-Online: Schäuble erwartet Anschlag mit schmutziger Bombe, 28.01.2006, http://www.spiegel.de/politik/deutschland/0,1518,397686,00.html

Störing Marc: „LG Konstanz: Zugriff auf Anonymisierungsserver“, in: MMR 2007 Heft 3 S. 194ff

Uhe Bianca, Herrmann Jens: Überwachung im Internet – Speicherung personenbezogener Daten auf Vorrat durch Internet Service Provider. Diplomarbeit. Berlin 2003, http://ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf

Winsemann Bettina: "2006 – da sind wir völlig machtlos", bei Telepolis, 20.02.2006, http://www.heise.de/tp/r4/artikel/22/22085/1.html