Michael Wettern

Umsetzung der Vorratsdatenspeicherung an den Hochschulen

„Nichts hören – nichts sehen, reicht nicht“

Vor dem Hintergrund aktueller Skandale im Umgang mit personenbezogenen Daten und dem anhaltenden Widerstand von kleineren IT-Unternehmen gegen die Vorratsdatenspeicherung skizziert der Verfasser die Argumentationen zur Umsetzungspflicht der Hochschulen zur Vorratsdatenspeicherung. Politische Entscheidungsvorgaben fehlen.

1 Datenschutzskandale

Das Jahr 2008 hat aus Sicht des Datenschutzes gute Chancen, in die Annalen einzugehen – als Jahr mit zuvor nicht für möglich gehaltenen Verstößen gegen den Datenschutz. Von Jahresbeginn an häuften sich Meldungen über Verstöße gegen die Vorgaben des seit gut einem viertel Jahrhundert gültigen Rechts auf informationelle Selbstbestimmung. Der Öffentlichkeit wurden heimliche Ausspähungen in verschiedenen Firmen mitgeteilt (u.a. Siemens, Lidl, Ikea, Burger King, Telekom), die mit ungeahnter krimineller Energie getätigt worden waren.[1]

Die Spitzel-Affäre der Telekom hat in der Zwischenzeit zu einer ersten Festnahme geführt: Gegen den früheren Leiter für interne Ermittlungen des Konzerns, der die Bespitzelung u.a. von Aufsichtsräten und Journalisten organisierte, wurde als Hauptverdächtiger ein Verfahren eröffnet.[2]

Prof. Dr. Michael Wettern

Technischen Universität Braunschweig, Datenschutzbeauftragter

E-Mail: m.wettern@tu-braunschweig.de

Die Bonner Staatsanwaltschaft ermittelt gegen mehrere Personen in dieser Affäre.[3] Gewerkschafter wurden durch den Konzern offenbar während heißer Tarifverhandlungen ausgespäht, nicht nur Verbindungsdaten sondern auch Informationen durch mehrere Einbrüche zusammen getragen. Die Anwältin der Arbeitnehmervertreter, die ehemalige Bundesjustizministerin Prof. Herta Däubler-Gmelin befürchtet noch weitere Enthüllungen in diesem Skandal. Der ehemalige FDP-Bundesinnenminister Gerhart Baum, Anwalt der ausgespähten Gewerkschaftler, geht davon aus, bisher nur die Spitze des Eisbergs gesehen zu haben.[4]

Gegenüber diesen Verstößen stellt sich die Datenpanne der Landesbank Berlin, ausgelöst durch den Heißhunger auf Christstollen, als eher kurios heraus.

Auch der Datenverlust der Kieler Karstadt-Filiale, der Kisten mit Belegen über Kreditkartenabrechnungen während der rasanten Fahrt eines DHL-Transporter auf der Autobahn abhanden kamen (teilweise vom Winde verweht), zeigen den enormen Nachholbedarf für einen gesicherten Transport von Datenmaterial. Während Geldtransporte erheblich geschützt sind, gilt dies nicht für Unterlagen mit durchaus sensiblen Daten wie Namen, Konto- und Kreditkarten, diese werden eher auf Kutschfahrten durch die Republik befördert.[5]

Ähnlich unsensibel gehen Hochschulen manchmal mit den Daten ihrer Studierenden um: sie lassen sich von Firmen nicht lange bitten und übermitteln diesen auf Nachfrage Daten ausgewählter Studierender eines Fachbereiches (Vordiplom nicht schlechter als mit der Note 2,3 abgelegt), ohne dafür die Einwilligung der Studenten zuvor eingeholt zu haben.[6] Der Fachbereich Wirtschaftwissenschaften der Freien Universität Berlin hat für eine entsprechende Anfrage dafür im Jahr 2007 sogar eine Einnahme verbucht: 280 Euro.[7]

2 Zwischen Politik und Karlsruhe

So beklagenswert diese Datenskandale auch sind, die Meldungen darüber haben einer breiten Öffentlichkeit die Bedeutung des Datenschutzes deutlich vor Augen geführt. Nicht zu unterschätzen für die öffentliche Wertschätzung des Datenschutzes sind ebenso die durch Bundesinnenminister Wolfgang Schäuble mehrfach ausgelösten Diskussionen über einige von der Bundesregierung geplanten Gesetzesänderungen.

1 Wettern, M. (2008) Zur Einhaltung des Datenschutzes an Hochschulen, DuD 7, S. 466-468

2 Leyendecker, H. (2008) Erste Festnahme nach Spitzelaffäre, Süddeutsche Zeitung, www.sueddeutsche.de/wirtschaft/142/451851/text

3 www.zeit.de/online/2008/51/telekom-festnahme

4 www.swr.de/report/presse/-/id=1197424/nid=1197424/did=4339828/7g81cd/index.html

5 Krempl, S. (2008) Datenpannen: LBB bleibt nach Wunder von Mainhatten in der Kritik, www.heise.de/newsticker/meldung/120788

6 Heiser, S. (2008) Unis verschenken Studentendaten, taz, 23. Dezember

7 Heiser, S. (2008) Die Uni schweigt, taz, 23. Dezember

Das Verfassungsgericht in Karlsruhe hat diese beabsichtigten Änderungen mehrfach bürgerfreundlich korrigiert (Entscheidung zur Online-Durchsuchung von privaten Computern, Erfassung von Autokennzeichen und zur Vorratsdatenspeicherung).[8]

Karlsruhe wird sich ein weiteres Mal mit Fragen des Datenschutzes befassen müssen, denn Gerhart Baum will eine Beschwerde gegen das BKA-Gesetz vor dem Bundesverfassungsgericht einreichen, nachdem der Bundespräsident das umstrittene Gesetz zwischen den Jahren unterschrieb.[9] Während sich die Bundesregierung bei der geplanten Vorratsdatenspeicherung für unangreifbar hält[10] und den Gegnern „systematische" Fehler vorwirft[11], fordern andere wie der „Chaos Computer Club" durch seine Sprecherin Constanze Kurz, aber auch Ulf Buermeyer, Richter am Landgericht Berlin, den von den Verfassungsrichtern zuerkannten absolut geschützten Kernbereich der privaten Lebensgestaltung auch für Datenträger zu gewähren.[12]

Gegen ständig neue Überwachungsgesetze argumentieren andere mit dem Hinweis, diese würden nicht den Terrorismus, sondern nur die Angst davor bekämpfen: statt Gesetze für Vorratsdatenspeicherung, Videoüberwachung und Bundestrojaner bräuchte es Anstrengungen, die Ursachen des Terrorismus mit Programmen gegen Jugendarbeitslosigkeit und Armut zu bekämpfen.[13]

3 Schutzmöglichkeiten

Sandro Gaycken setzt sich für den Datenschutz ein, um technische Verfahren sicher zu machen und um zu vermeiden, dass sensible Daten kursieren. Er hält treffend fest, dass gegenwärtig der Datenschutz in Deutschland das informationelle Selbstbestimmungsrecht nicht effizient sichern kann, da er Datenschutzverletzungen wegen mangelnder Ausstattung (Sach- und Personalmittel) und fehlenden Sanktionsmöglichkeiten nicht abwehren kann.[14]

Die informationelle Selbstbestimmung soll eine freie, informierte Entscheidung ermöglichen, was ein Verständnis möglichst aller relevanten Einzelheiten dazu notwendig macht. Aktuelle Überwachungssysteme erschweren dies aber erheblich oder machen es unmöglich. Wer weiß schon noch, wann er in welcher Form persönliche Informationen an wen weitergegeben hat. Der schleichenden Entblößung, der bisweilen ungehemmten Weitergabe persönlicher Daten, scheint das Ende der Privatsphäre[15] zu bedeuten.

Es kommt auf eine ausgewogene Balance an zwischen Freiheit und Sicherheit, denn die informationelle Selbstbestimmung ist ein Bestandteil persönlicher und kommunikativer Freiheit und damit zugleich ein Definitionsmerkmal der Rechtsstaatlichkeit[16] (der Zweck des Staates ist die Wahrung der Freiheit[17]).

Der Präsident des Bundesverfassungsgerichts, Hans-Jürgen Papier, mahnte daher alle Bürger eindringlich, der eigenen Privatsphäre und Persönlichkeit wieder stärkeres Gewicht beizumessen: jeder Einzelne ist seiner Meinung nach zum sorgsamen Umgang mit persönlichen Daten gefordert.[18]

Der Gerichtspräsident, seit elf Jahren als zunächst konservativer Staatsrechtler mit CSU-Parteibuch am Bundesverfassungsgericht tätig, ist inzwischen überzeugter Datenschützer und Bürgerrechtler.[19] Er rief den Gesetzgeber auf, bei der Bekämpfung und Verhinderung von Kriminalität die Gewichte von Freiheit und Sicherheit nicht grundlegend zu verschieben und sich vor allem um die Gefahren der von Privaten gespeicherten Informationen zu kümmern – aber er rief eben auch dazu auf, dass jeder Bürger in Selbstverantwortung mit den eigenen Daten umzugehen hat.

4 Vorratsdatenspeicherung

Ab dem 1. Januar 2009 gilt eine deutlich erweiterte Vorratsdatenspeicherung. Während Verbindungsdaten von Festnetz- und Mobil-Telfongesprächen bereits seit Beginn 2008 gespeichert werden müssen[20], sind gewerbsmäßige Anbieter nun verpflichtet, Verbindungsdaten zum Versandt von E-Mails, aber auch Internet-Einwahlvorgänge und Internet-Telefonie für sechs Monate zu speichern. Gespeichert werden muss, wann wer mit wem wie lange kommuniziert hat. Zuwiderhandlungen sind mit Bußgeldern bis zu 500.000 Euro belegt.[21]

Im Rahmen einer Sammelklage haben rund 34.000 Personen Verfassungsbeschwerde eingelegt, was zwar nicht zu einer Aufhebung der Speicherungspflicht geführt hat, jedoch die Nutzung der Daten bis zum endgültigen Urteil für die Aufklärung schwerer Straftaten beschränkt. Einige kleine Firmen sind von dieser Speicherverpflichtung entbunden.

So hat das Berliner Verwaltungsgericht die deutsche Tochter der „British Telecom" im Oktober 2008 vorerst von der Vorratsspeicherung entbunden – wogegen die Bundesregierung Beschwerde eingelegt hat, über die noch nicht entschieden ist.[22]

Ein weiterer ähnlicher Fall muss in Karlsruhe entschieden werden: Die Berliner Firma „Cable and Wireless" will ohne finanzielle Entschädigung die für die Überwachung notwenige Technik nicht anschaffen. Zwar wird die staatliche Überwachung für die Firmen finanziell bald erträglicher, denn die Einrichtung einer Telefonüberwachung soll demnächst mit 100 Euro vergütet werden, so sieht es die geplante Neuregelung des Justizvergütungs- und Entschädigungsgesetzes vor, zusätzlich werden auch noch anfallende Leitungskosten pauschal gezahlt. Die Pau-

8 Kerscher, H. (2009) Klug, klüger, Karlsruhe?, Süddeutsche Zeitung, 2. Januar

9 Baums Beschwerde, Braunschweiger Zeitung, 30.12.2008

10 www.heise.de/newsticker/meldung/121089

11 www.heise.de/ct/hintergrund/meldung/121088

12 Schwan, B. (2008) Die Verletzung der digitalen Persönlichkeit muss gestoppt werden – Intimsphäre auf Festplatte, taz, 29. Dezember

13 Biermann, Kai (2008) Zu viel des Guten, Zeit online, www.zeit.de/online/2008/52/terror-angst

14 „Informationelle Selbstbestimmung stirbt", www.zeit.de/online/2008/informationelle-selbstbestimmung; Gaycken, S. (2008) Die Vergeistigung des Technotops. Neue Gefahren in einer neuen technischen Situation. In: S. Gaycken und C. Kurz (Hrsg.) 19884.exe, ISBN 978-3-89942-766-0, S. 25-44

15 Schaar, P. (2007) Das Ende der Privatsphäre, C. Bertelsmann, ISBN 978-3-570-00993-2

16 Bielefeldt, H. (2008) „Ich habe nichts zu verbergen" – ein gedankenloser Spruch, Datenschutz Nachrichten, Heft 1, S. 8-10.

17 Papier, H.-J. (2008) Der Zweck des Staates ist die Wahrung der Freiheit – Über das Spannungsverhältnis von Freiheit und Sicherheit aus verfassungsrechtlicher Sicht. Ein Vortrag auf der Tagung ´Freiheit und Sicherheit – Verfassungspolitische Dimensionen der Akademie für Politische Bildung Tutzing am 30. Mai 2008´, Die Welt, 02.06.2008.

18 www.sueddeutsche.de/computer/899/451610/text; www.abendblatt.de/daten/2008/12/23/996593.html

19 Kerscher, H. (2009) Klug, klüger, Karlsruhe?, Süddeutsche Zeitung, 2. Januar

20 Auch Internet-Daten werden nun gespeichert, Süddeutsche Zeitung, 24.-26.12.2008

21 Rath, C. (2008) Datenspeicherung geht 2009 erst richtig los, taz, 31. Dezember

22 Rath, C. (2009) Staat lässt sich Überwachung was kosten, taz, 2. Januar

schalen werden jedoch nur fällig, wenn die Polizei auch Daten angefragt hat. Da verschiedene Anbieter jedoch nur Geschäftskunden und keine Endverbraucher bedienen, würden zwar die teuren Überwachungssysteme finanziert werden müssen, jedoch selten durch die Polizei genutzt.

Bestärkt durch den Beschluss des Berliner Verwaltungsgerichts haben einige kleinere Internetprovider angekündigt, der Pflicht zur Vorratsdatenspeicherung von Verbindungs- und Standortdaten nicht nachkommen zu wollen.[23]

So hat die Firma „Manitu" die Bundesnetzagentur aufgefordert, das Unternehmen ebenfalls von der sechsmonatigen Vorratsdatenspeicherung zu befreien. Im Rahmen des internationalen Aktionstages „Freedom not Fear" haben zuvor bereits 36 kleine Provider aus Europa erklärt, die europa-weiten Vorgaben zur Vorratsdatenspeicherung boykottieren zu wollen. Unter anderem wollen „Espace4you", „Nadir.org", „Samizdat.net" oder „Systemausfall.org" nicht zu „inoffiziellen Polizeimitarbeiter" werden.

Firmen kritisieren vor allem, nur pauschale Entgelte für die Betriebskosten der Überwachung zu erhalten, aber keine Erstattung der zuvor notwendigen Investitionen, die nach Angaben von Verbänden der Telekom-Unternehmen ca. 75 Millionen Euro, bei der Internet-Branche sogar über 300 Millionen Euro betragen sollen.[24]

5 Vorratsdaten an den Hochschulen

Für die Hochschulen der Bundesrepublik erscheint die Lage zur Vorratsdatenspeicherung zur Zeit noch unübersichtlich.

Zwar ist seit Anfang Januar 2008 das Gesetz zur Neuregelung der Telekommunikationsüberwachung (TKG) und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG in Kraft getreten, das in § 113 a TKG eine Speicherfrist von Verkehrsdaten für die Dauer von sechs Monaten vorsieht.[25] Das betrifft nur Anbieter, die öffentlich-zugängliche Telekommunikationsdienste erbringen. *Hochschulen sind von der Verpflichtung der Vorratsdatenspeicherung aufgrund ihres geschlossenen Benutzerkreises ausgenommen, so die Begründung im Regierungsentwurf.*[26] Damit fehlt eine Erlaubnis zur Speicherung von Verbindungsdaten über den zur Aufrechterhaltung der Telekommunikation erforderlichen Zeitraum hinaus (dieser umfasst regelmäßig 7 Tage).[27]

Nach gegenwärtigem Recht gilt die Pflicht zur Vorratsdatenspeicherung von Verkehrsdaten nicht für Hochschulen, jedenfalls nicht für diejenigen, die ausdrücklich nur eine *dienstliche Nutzung* der hochschuleigenen IT-Infrastuktur zugelassen haben. Trifft das gleichermaßen auch auf Hochschulen zu, die entweder konkludent, als über Jahre geübte Praxis, oder ausdrücklich ihren Studierenden und dem Personal neben der dienstlichen auch die *private Nutzung* eingeräumt haben?

Zwar wird in diesen Fällen damit Endverbrauchern die IT-Nutzung der Hochschuleinrichtungen gestattet – allerdings gilt dies immer noch für einen geschlossenen Nutzerkreis, ermöglicht ist die private Nutzung ausschließlich den Studierenden und dem Personal von Hochschulen. Solange die Hochschulen somit nicht-öffentlich zugänglich Telekommunikationsdienste anbieten, solange entfällt damit die Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten – so ließe sich trefflich argumentieren.

Eine andere Argumentation unterstellt bei dauerhaft konkludenter oder auch ausdrücklich eingeräumter privater Internetnutzung durch Studierende und Personal ein geschäftsmäßiges Angebot von Telekommunikationsdiensten durch Hochschulen. Nach § 3 Nr. 10 TKG genügt dazu bereits ein nachhaltiges Angebot, eine Gewinnerzielungsabsicht (gewerblicher Charakter) muss mit der Zustimmung zu privater Nutzung nicht notwendigerweise verbunden sein. Damit wäre die Pflicht zur sechsmonatigen Vorratsdatenspeicherung von Verkehrsdaten auch durch diese Hochschulen zu gewährleisten, verbunden mit einem erheblichen finanziellen Aufwand zur Einrichtung der dafür notwendigen Systeme.

Diese Argumentation steht allerdings im Widerspruch zur Begründung des Gesetzentwurfes durch die Bundesregierung (siehe Fn. 26) und erscheint daher verworfen werden zu können.

Im Zweifelsfall werden Juristen diese Fragen in Zukunft zu klären haben. Die mit der Vorratsdatenspeicherung verbunden Kosten (siehe weiter vorne) legen die Vermutung nahe, dass Hochschulen auch bei privater Nutzung der IT-Infrastruktur durch Studierende und Beschäftigte von dieser Speicherpflicht entbunden sein werden. Für die Bundesländer als Träger von Hochschulen in staatlicher Verantwortung (Stiftungs-Universitäten seien an dieser Stelle nicht berücksichtigt) entstünden ansonsten gegenwärtig kaum kalkulierbare Kosten, ein Verbot der privaten Nutzung ließe sich andererseits kaum durchsetzen.

Es bleibt zu wünschen, dass diese grundsätzlichen Fragen zukünftiger IT-Gestaltung und IT-Nutzung über den Tellerrand von Hochschulen hinaus diskutiert zu einem gesellschaftlichen Konsens führen und nicht wie häufig ausgesessen werden durch nichts sehen – nichts hören – ja nicht drüber reden.[28]

Die den Hochschulen übergeordneten Fachministerien der Länder üben sich in diesen Fragen seit Monaten in Zurückhaltung, zielorientierte Vorgaben sind gegenwärtig nicht zu erkennen.

23 Krempl, S. (2008) Provider bei der Vorratsdatenspeicherung zwischen allen Stühlen, http://www.heise.de/newsticker/Provider-bei-der-Vorratsdatenspeicherung-zwischen-allen-Stuehlen--/meldung/119575

24 Rath, C. (2009) Staat lässt sich Überwachung was kosten, taz, 2. Januar

25 Die Pflicht zur Speicherung von Verbindungsdaten ist geregelt in TKG § 113 a Abs. 1 Satz 1, er lautet: „Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern."

26 Da die Telekommunikationsdienste von Universitäten nicht öffentlich zugänglich sind, sind sie von dieser Speicherpflicht nicht betroffen.
Die Bundesregierung verweist ausdrücklich in der Begründung ihres Gesetzesentwurfes auf diese Ausnahme (siehe S. 161 der Begründung http://www.bmj.bund.de/files/-/2047/RegE%20TK%DC.pdf): „Zu Absatz 1: Absatz 1 Satz 1 beschreibt den Kreis der zur Speicherung Verpflichteten. Danach richten sich die Speicherungspflichten an diejenigen, die öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringen. Daraus folgt zugleich, dass für den nicht öffentlichen Bereich (z. B. unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für dort immatrikulierte Studierende oder Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen) eine Speicherungspflicht nicht besteht."

27 Urteil des LG Darmstadt vom 06.06.2007 (Az.: 10 O 562/03 – Kurzfristiges Speichern von I-Adressen); Urteil des AG Bonn vom 05.07.2007 (Az.: 9 C 177/07 – Kurzfristiges Speichern von I-Adressen); Zusammenfassender Überblick siehe: Kaufmann, N. (2008) Rechtssprechung zum Datenschutz 2007, DuD 248-257.

28 Minkmar, N. (2008) Nichts sehen. Nicht hören. Ja nicht darüber reden. Das „deutsche Problem" gibt es wirklich. Es heißt: Stillstand. Wir machen es uns gerade so richtig gemütlich in der Krise. FAZ Sonntagszeitung, 28. Dezember

6 Notwendigkeit eines Arbeitnehmerdatenschutzgesetzes

Nach den veröffentlichten datenschutzrechtlichen Verstößen verschiedener Firmen des vergangenen Jahres haben zu Beginn des Jahres 2009 Bespitzelungen der Deutsche Bahn AG das Licht der Öffentlichkeit erblickt, die durchaus als Rasterfahndung bezeichnet werden können.[29]

Bahnchef Mehldorn räumte scheibchenweise ein, zur Korruptionsbekämpfung eine Detektei (Network Deutschland GmbH, deren Expertise auch die Telekom in Anspruch nahm) mehrfach beauftragt zu haben, Datenbestände von Mitarbeiterinnen und Mitarbeiter mit etwa 80.000 Lieferfirmen der Bahn abzugleichen. Es wurden immer wieder sensible Daten und E-Mails von Mitarbeitern und zum Teil auch deren Angehörigen durchleuchtet, in einzelnen Projekten auch der Lebensstil der Betroffenen untersucht.[30]

Als letzte Offenbarung räumte die Bahn in einem als „Zwischenbericht" bezeichneten Bericht[31] ein, neben den drei bisher bekannten Abgleichungen zwei weitere, bisher nicht veröffentlichte, in den Jahren 1998 und 2005/2006, durchgeführt zu haben. Es darf getrost unterstellt werden, dass nun wirklich die gesamte Belegschaft der Bahn überprüft wurde (rund 240.000 Beschäftigte).[32]

Zum keinem Zeitpunkt der Überprüfung waren weder die Personalvertretung noch der Datenschutzbeauftragte der Bahn über die Aktionen informiert. Die völlige Unverhältnismäßigkeit dieser Überprüfungen zeigt deutlich, dass es der Bahn nicht nur um Korruptionsbekämpfung gegangen sein kann, sondern auch um das Offenlegen von Kommunikationswegen und Informationssträngen, die unkontrolliert durch den Bahnchef das Bahngelände verlassen.[33] Datenschützer aber auch die Politik warnten vor „Unternehmer-Selbstjustiz" und forderten Abhilfe durch eindeutige Gesetze.[34]

Deutlich zeigt sich an den Massenüberprüfungen das seit Jahren fehlende Arbeitnehmerdatenschutzgesetz.

Bestandteil dieses Gesetzes sollte ein „Datenbrief" sein, wie er von dem scheidenden Landesdatenschutzbeauftragte von Baden-Würtemberg, Peter Zimmermann, aber auch von Constanze Kurz vom Chaos Computer Club, seit langem gefordert wird.[35] die jährliche Auflistung von Firmen und Behörden für Bürgerinnen und Bürger über die über sie gespeicherten Daten und deren Zweckbindung.

Vor allem muss das Arbeitsnehmerdatenschutzgesetz Regelungen enthalten, die eine Durchsetzung des Datenschutzrechts ermöglichen und Verstöße dagegen mit deutlichen Strafen belegen. Diese Vorgaben sollten ohne Abstriche auch für Hoch-schulen gelten.

29 Rother, R. (2009) Die Spitzel-Bahn, taz, 29. Januar

30 Kosch, S. (2009) Es wird langsam eng für Mehdorn, taz, 3. Februar

31 Vorstand der Deutschen Bahn AG und Chief Compliance Officer (2009) Zwischenbericht – Überprüfung der Ordnungsmäßigkeit von Maßnahmen der Korruptionsbekämpfung in den Jahren 1998-2007, Potsdamer Platz 2, 10785 Berlin, 10. Februar

32 Zeit online (2009) Neue Vorwürfe – Deutsche Bahn überprüfte alle Mitarbeiter, 3. Januar; Zeit online (2009) Mehdorn gesteht noch mehr Spitzel-Aktionen, 10. Februar

33 Spiegel online (2009) Politiker werfen Bahn Jagd auf Informanten vor, 31. Januar

34 Zeit online (2009) Schaar verlangt Gesetze gegen Bespitzelung, 4. Januar

35 Lee, F. (2009) Sammelwut soll transparent werden, taz, 4. Februar