Ulrich Greveler

Post-Privacy

Hat weniger Datenschutz mehr Zukunft?

Ein Sachbearbeiter des Landesbeauftragten für Datenschutz in Niedersachsen forderte 2011 einen Betreiber eines deutschen Webforums auf, eine „Datenverarbeitungsverfahrensbeschreibung für das Verfahrensregister beim Datenschutzbeauftragten“ zu erstellen (Bleich, 2011). Was zunächst nur nach missglückter Amtssprache klingt, hatte es in sich: Der Betreiber wurde gedrängt, Werbeanzeigen aus seinem kostenfreien Forum zu entfernen, da über die geschalteten Anzeigen personenbeziehbare Daten (hier: dynamisch zugewiesene IP-Adressen) zu den Werbedienstleistern in den Vereinigten Staaten übermittelt wurden. Ist die Sorge um die Datenschutzbelange der Bürger hier noch gerechtfertigt – oder liegt hier bereits ein mangelndes technisches Verständnis des Internets vor, das ohne zumindest kurzzeitige Speicherung von IP-Adressen nicht mehr funktionsfähig wäre? Könnten Datenschützer dann die gesamte Netzkommunikation unterbinden? Um diese Fragen drehte sich die anschließende Diskussion in den Netzforen.

Anfang 2011 trat als Gegenpol zur Datenschützerbürokratie die „datenschutzkritische Spackeria“ in die Öffentlichkeit, die seitdem ein loses Mitmachprojekt rund um die Diskussion zum Begriff „Post-Privacy“ darstellt. Mit der Mitgründerin und Piratin Julia Schramm, die im März 2011 ein viel beachtetes spiegel.de-Interview gegeben hatte (Reißmann, 2011), bekam die Gruppe ein Gesicht und mediale Aufmerksamkeit. Post-Privacy wurde von Schramm nicht als normativer Anspruch festgelegt, sondern als ein persönlicher Anspruch derjenigen, die ihre Privatsphäre selbst definieren und Datenschützern keine Macht darüber geben wollen, was öffentlich ist und was privat zu sein hat. Formuliert wurde im Interview zudem die „Idealvorstellung einer Gesellschaft, die Privatsphäre nicht mehr nötig hat, weil es keine Diskriminierung mehr gibt“. Vertreter der Spackeria merkten zudem an, dass Datenschutz in seinen Regelungen veraltet ist und missbraucht wird, um Intransparenz zu befördern; dies ist im Kontext politischer Forderungen der Piratenpartei, die Transparenz bei politischen Entscheidungsprozessen als

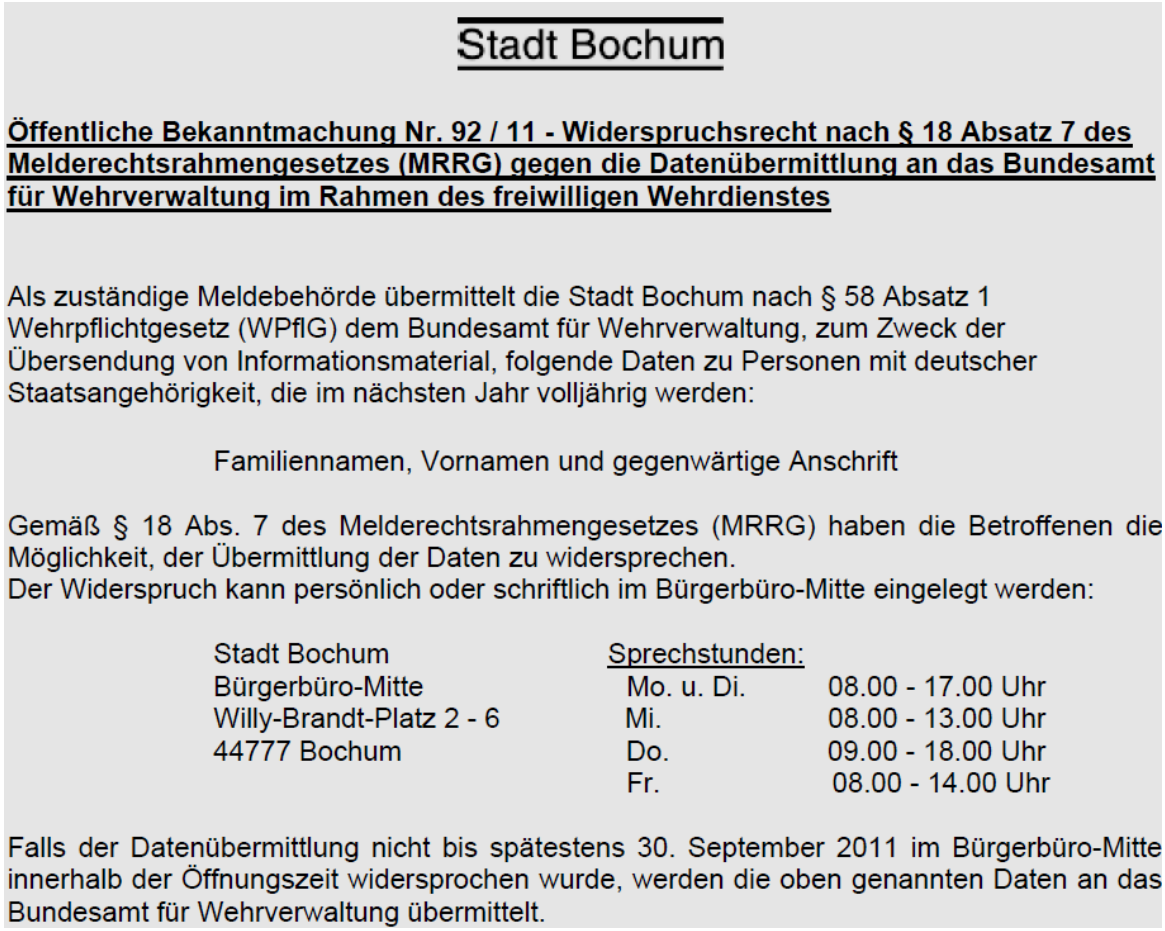
Kernthema formuliert, auf Resonanz, aber auch auf heftige Kritik gestoßen. Die provokante Rhetorik, die die Spackeria über ein Blog[1] verbreitet, führte mehrfach zum Vorwurf der Naivität; insbesondere wurde der Gruppe unterstellt, sie verstehe nicht, dass Datenschutz ein zentrales Abwehrrecht des Bürgers gegen den Staat darstelle. Eine Debatte über den Status quo des Datenschutzes und die Anpassung seiner Normen an eine Gesellschaft, in der Post-Privacy weit mehr eine Zustandsbeschreibung als eine Forderung ist, war jedoch überfällig.

Denn auch wenn es einen breiten Konsens darüber gäbe, dass Privacy richtig (und wichtig) ist, würde das nicht bedeuten, dass der vorhandene Datenschutz stets Gutes bewirkt, und erst recht nicht, dass viel Datenschutz besser für die Bürger ist als wenig Datenschutz. Der weitreichende Datenschutz in Deutschland wird nicht selten als Exportschlager angesehen, als vorbildlich für Europa (Europäische Kommission, 2011) und die westliche Welt. Hier wäre mehr Bescheidenheit angebracht: Denn Datenschutz in Deutschland ist nicht nur weitreichend, er ist auch bürokratisch, er ist auch fehlgeleitet und übertrieben – und er hat große blinde Flecken! Insbesondere ist er in seinen Kompetenzen zu wenig technisch und als Disziplin insgesamt zu sehr juristisch.

1 Datenschützer schützen keine Daten – sie sorgen nur dafür, dass Opfer wirksam einwilligen

Ein Beispiel aus dem Jahr 2012: Der Autor war auf einer Tagung, die Probleme in Bezug auf Datenschutz und -sicherheit in großen Unternehmen beleuchtete. Eine Referentin, Datenschutzbeauftragte eines Energieversorgers, gab ihren anwesenden Kollegen wertvolle Tipps: Wie kann die private Nutzung von E-Mails wirksam verboten werden? (Nach dem Grund für ein Verbot wurde nicht gefragt.) Welche Betriebsvereinbarung wird benötigt, um die E-Mails von Beschäftigen kontrollieren zu können? (Der Text wurde bereitgestellt.) Wie führt man die Kontrolle weitgehend ohne Rechtsverstöße durch? (Genannter Tipp: Nur am Endgerät kontrollieren, dann ist Artikel 10 Grundgesetz – also hier das Fernmeldegeheimnis – elegant umgangen). Die Datenschutzbeauftragte ist Juristin und daher kompetent, die rechtlichen Fragen zu beantworten. Aber welches Selbstverständnis eines Datenschützers im Unternehmen steckt hinter diesen Aktivitäten? Schützt man Daten dadurch, dass sich Opfer von Schnüffeleien aufgrund rechtswirksam gegebener Zustimmungen nicht mehr wehren können?

[1] http://blog.spackeria.org/



Stadt Bochum

Öffentliche Bekanntmachung Nr. 92 / 11 - Widerspruchsrecht nach § 18 Absatz 7 des Melderechtsrahmengesetzes (MRRG) gegen die Datenübermittlung an das Bundesamt für Wehrverwaltung im Rahmen des freiwilligen Wehrdienstes

Als zuständige Meldebehörde übermittelt die Stadt Bochum nach § 58 Absatz 1 Wehrpflichtgesetz (WPflG) dem Bundesamt für Wehrverwaltung, zum Zweck der Übersendung von Informationsmaterial, folgende Daten zu Personen mit deutscher Staatsangehörigkeit, die im nächsten Jahr volljährig werden:

Familiennamen, Vornamen und gegenwärtige Anschrift

Gemäß § 18 Abs. 7 des Melderechtsrahmengesetzes (MRRG) haben die Betroffenen die Möglichkeit, der Übermittlung der Daten zu widersprechen.
Der Widerspruch kann persönlich oder schriftlich im Bürgerbüro-Mitte eingelegt werden:

Stadt Bochum	Sprechstunden:	
Bürgerbüro-Mitte	Mo. u. Di.	08.00 - 17.00 Uhr
Willy-Brandt-Platz 2 - 6	Mi.	08.00 - 13.00 Uhr
44777 Bochum	Do.	09.00 - 18.00 Uhr
	Fr.	08.00 - 14.00 Uhr

Falls der Datenübermittlung nicht bis spätestens 30. September 2011 im Bürgerbüro-Mitte innerhalb der Öffnungszeit widersprochen wurde, werden die oben genannten Daten an das Bundesamt für Wehrverwaltung übermittelt.

Abb. 1: Bekanntmachung der Stadt Bochum, 2011

Eine ähnliche Datenschützer-Mentalität kann man unterstellen, wenn man die öffentliche Bekanntmachung der Stadt Bochum (hier nur exemplarisch herausgegriffen) sieht, die die Weitergabe von Adressdaten junger Volljähriger an das Bundesamt für Wehrverwaltung ermöglicht (Abb. 1). Diese Daten werden offenbar zu Werbezwecken bei der Rekrutierung Freiwilliger verwendet. Eine Weitergabe der Adressen von der Kommune an ein Bundesamt erscheint als niederschwelliger Eingriff in die informationelle Selbstbestimmung der Betroffenen. Aber die Datenschutzbeauftragten könnten sich hier positionieren: Entweder, die Weitergabe ist unkritisch (dann kann man auf die teuren Bekanntmachungen verzichten), oder eine Zustimmung ist aufgrund des Eingriffs erforderlich (dann sollte man auch jeden Betroffenen fragen!). Die öffentliche Bekanntmachung macht aus einer Datenschutzverletzung eine rechtlich wasserdichte Vorgehensweise, obwohl die Behörde annehmen kann, dass die Zielgruppe höchst selten die amtlichen Bekanntmachungen in der Tageszeitung liest. In dem Fall hat der Datenschutzbeauftragte aber seine Aufgabe verfehlt: Es wurden keine Daten geschützt, lediglich die Zustimmungsakrobatik ist um einen weiteren Salto bereichert worden.

Eine Lösung wäre hier naheliegend: Die Werbebroschüren sind wohl kaum personalisiert: sie könnten also auch den Kommunen stapelweise zum Weiterversand an die Zielgruppe überstellt werden. Vermutlich ist die Weiterberechnung der Versandkosten zwischen den öffentlichen Stellen aber komplizierter als die rechtssichere Umgehung des Datenschutzes.

2 Regierungen benötigen nicht mehr Daten als Oppositionen

Datenschutz wird oft als bürokratisch wahrgenommen; und tatsächlich ist er zur Allzweckwaffe der Bürokratie verkommen. Aber welche Datenschützer wehren sich öffentlich, wenn Datenschutz als Ausrede benutzt wird? Ein Beispiel: Die Bundesregierung verweigerte der Opposition Einsicht in die Berechnung der Hartz-IV-Sätze – aus Datenschutzgründen (n-tv, 2010)! Obwohl die Oppositionsparteien Rechenfehler in einem Papier des Bundesarbeitsministeriums aufgedeckt hatten, erhielten sie keine detaillierten Zahlen zu Verbrauchsausgaben erfasster Haushalte. Details wären nicht mehr hinreichend anonym. Mit diesem Datenschutz-Argument (Eine Weitergabe von Statistiken über eine geringe Zahl von Haushalten sei „aus datenschutzrechtlichen Gründen nicht möglich“, so der Ministeriumssprecher) kann sich eine Regierung wirksam der Kontrolle entziehen. Hier wird der Datenschutz, allgemein als Abwehrrecht gegen den Staat aufgefasst, auf den Kopf gestellt. Die (ohnehin fragwürdige) Begründung sollte für den Datenschutzbeauftragten Anlass genug sein, einzuschreiten. Die Opposition darf Einblicke in die Arbeit der Geheimdienste und des Militärs nehmen, Mitglieder im parlamentarischen Kontrollgremium werden zur Verschwiegenheit verpflichtet; nur die Nachberechnung von Hartz-IV-Sätzen scheitert angeblich an den Datenschutzinteressen der Betroffenen?!
Es gibt weitere erschütternde Beispiele: Patienten werden nicht darüber informiert, dass sie fehlerhafte Prothesen erhielten (ein Register „scheiterte am Geld und am Datenschutz“; Ludwig, Mertin & Schmid, 2011). Firmen, die bei der Herstellung von Gammelfleisch erwischt wurden, sollen aus Datenschutzgründen nicht genannt werden (Heckmann, 2006).
Welche politische Forderung könnte man aus diesen Fällen ableiten? Mindestens eine: Die Instrumentalisierung des Datenschutzes soll gleichermaßen scharf verfolgt werden wie seine Verletzungen.

Bundesland	Landesbeauftragte(r) für den Datenschutz	Qualifikation
Baden-Württemberg	Jörg Klingbeil	Jurist
Bayern	Thomas Petri	Jurist
Berlin	Alexander Dix	Jurist
Brandenburg	Dagmar Hartge	Juristin
Hamburg	Johannes Caspar	Jurist
Hessen	Michael Ronellenfitsch	Jurist
Mecklenburg-Vorpommern	Reinhard Dankert	Diplomingenieur
Nordrhein-Westfalen	Ulrich Lepper	Juristin
(…)		

Tabelle 1: Landesdatenschutzbeauftragte und ihre fachlichen Qualifikationen (Stand: Juni 2012)

3 Datenschützer sollten sich mit Daten und ihrem Schutz auskennen

Datenschutzfragestellungen werden in Deutschland überwiegend als rechtliche Fragestellungen angesehen; und natürlich ist der Datenschutzbeauftragte dann ein Jurist (Tab. 1), denn wer sonst sollte die komplexe juristische Materie durchschauen? Tatsächlich beschränkt sich die Prüfung insbesondere bei betrieblichen Datenschutzbeauftragten oft allein auf die beiden juristischen Fragen: Ist ein Datum personenbezogen? (Sonst ist der Datenschutzbeauftragte nicht zuständig.) Gibt es eine Rechtsgrundlage zur Speicherung? (Ggf. muss irgendwo ein Unterschriftenfeld mit der Einwilligung zur Speicherung eingepflegt werden und „geeignete Maßnahmen zum Schutz der Daten“ vorgesehen werden. Dann ist das „Datenschutzproblem“ gelöst.) Wichtiger wäre es aber, eine Einschätzung vornehmen zu können, wie sensibel die Daten sind, insbesondere welche Folgen eine Verarbeitung der fraglichen Daten für die Betroffenen haben kann. So ist die Angabe des Geschlechtes bei einem Datensatz, der Namen und Anschriften enthält, unzweifelhaft ein personenbezogenes Datum, kann aber in den meisten Fällen auch ohne Erhebung aus dem Vornamen erschlossen werden. Eine dynamisch zugewiesene IP-Adresse hingegen wird noch von vielen Gerichten als nicht personenbeziehbar angesehen, obwohl es

Millionen Singlehaushalte gibt und es bei Mehrgenerationenhäusern – selbst unter Beachtung von Antidiskriminierungs-Geboten – eher abwegig erscheint, Online-Egoshooter der 92jährigen Großmutter zuzuordnen. Auch die Erhebung von Personennamen ist differenziert zu bewerten: Wenn der Namensträger das Privileg hat, weltweit eindeutig anhand der Kombination Vor- und Zuname identifizierbar zu sein, hat eine Veröffentlichung unter Namensnennung im Web erhebliche Konsequenzen, die ein Hansi Müller nicht befürchten muss. Im Einzelfall müssten bei einer Bewertung von Datenschutzaspekten die informatischen Begriffe Primär-, bzw. Fremdschlüssel, Verknüpfungsrelation und *Knowledge Discovery* eine Rolle spielen. Es ist aber zweifelhaft, dass dies über die Prüfung der (vorgeblichen) Personenbezogenheit hinaus in der Praxis geschieht.

Der technische und organisatorische Schutz der Daten muss in Beziehung zur Sensibilität der Daten gesetzt werden. Hier sind Kompetenzen zu Authentisierungsprotokollen, Kryptographie, vertrauenswürdiger Hardware, Seitenkanälen etc. hilfreich, die im klassischen Datenschutzumfeld eher schwach vertreten sind. Dazu ein Beispiel: Ein Abruf der Broschüre „Schützen Sie Ihre Daten. 10 Tipps zur Datensicherheit“ beim Landesbeauftragten für Datenschutz in NRW (2006) förderte (noch im Mai 2012) den Hinweis zutage:

> Es gibt unterschiedliche Verfahren, Daten sicher zu verschlüsseln. Allen gemeinsam ist das Prinzip, dass die einzelnen Buchstaben und Ziffern der Daten mit Hilfe eines Schlüssels (…) so oft vertauscht und durch andere Zeichen ersetzt werden, bis es praktisch unmöglich ist, ohne Kenntnis des Schlüssels (Geheimcodes) die Daten zu lesen.

Das ist zwar nicht falsch; es fehlt aber jeder praktische Hinweis auf Verfahren, Standards oder auch nur auf Weblinks, die dem Bürger Wege zu Verschlüsselungssoftware aufzeigen. Es wurde beim Tipp sogar versäumt, darauf hinzuweisen, überhaupt eine Software für den genannten Zweck zu benutzen. Der Leser könnte nach dem Lesen der Broschüre auf die Idee kommen, Buchstaben und Ziffern selbst händisch zu vertauschen, um Datenschutz zu erreichen. Ausführlicher hingegen ist die Information bei der (angeblich) datenschutzgerechten Verwendung von Faxgeräten:

> Sensible personenbezogene Daten (beispielsweise medizinische Daten) dürfen nur im Ausnahmefall unter Einhaltung zusätzlicher Sicherheitsvorkehrungen per Fax übertragen werden. So sind insbesondere mit der Empfängerin und dem Empfänger der Sendezeitpunkt und das Empfangsgerät abzustimmen, damit das Fax direkt entgegengenommen werden kann und vor der Einsichtnahme Dritter geschützt ist. (Landesbeauftragter für Datenschutz und Informationsfreiheit NRW, 2007)

Pointiert zusammengefasst: Wenn hochsensible Daten leichtsinnigerweise unverschlüsselt übertragen werden, sollten sie wenigstens nicht allzu lange im Faxgerät auf Abholung warten.

4 Wären Informatiker die besseren Datenschützer?

Die zuvor genannten Fälle illustrieren, dass die juristische Beurteilung von „Datenschutzproblemen“ bzw. die dafür formulierten „Lösungen“ wesentliche Ziele des Datenschutzes – insbesondere informationelle Selbstbestimmung und Schutz der Privatsphäre – unterlaufen können. Anstatt sich an der juristischen Frage nach der Personenbezogenenheit und der Einwilligung festzubeißen, könnten Informatiker stärker beleuchten, welche Eingriffe in die Privatsphäre tatsächlich aus den zu beurteilenden Daten bei einer missbräuchlichen Weiterverarbeitung konstruiert werden können, ob die Daten, in Abhängigkeit davon, wie kritisch sie sind, technisch angemessen geschützt werden und ob die Verarbeitung von Daten, die nicht oder nicht zweifelsfrei personenbezogen sind, trotz dieser Klassifizierung das Prinzip der informationellen Selbstbestimmung verletzen können, weil Verknüpfungen mit anderen Datenquellen oder erfolgreiches Data Mining algorithmisch möglich bleiben.

Dass Informatiker bei technisch und algorithmisch orientierten Fragestellungen im Allgemeinen kompetenter sind als Juristen, ist aber eine triviale Feststellung. Es wäre zu einfach, daraus zu folgern, dass Datenschutzbeauftragte in erster Linie eine Informatikkompetenz nachweisen müssten; denn bei der Beurteilung der Sensibilität von Daten spielen weitere nicht-technische und nicht-juristische Kriterien ebenfalls eine Rolle: Beispielsweise fiele die Beurteilung eines Tabubruchs oder der Verletzung einer sozialen Norm, die auf Grundlage personenbezogener Daten offenbar würde, in die Domäne von Soziologen oder Sozialpsychologen. Diese können aufgrund ihrer Expertise vermutlich eher einschätzen, ob eine Bloßstellung des Betroffenen von einer gewissen Erheblichkeit ist und folglich besondere Schutzmaßnahmen erforderlich sind. In besonderen Fällen könnten auch weitere kulturwissenschaftliche Disziplinen (z. B. Ethnologie) hilfreich bei der Beurteilung sein, wie kritisch und sensibel personenbezogene Daten sind. Die Liste lässt sich fast beliebig fortsetzen.

Der ideale Datenschützer ist demnach ein Allrounder, der technische, soziologische und psychologische, aber auch juristische Kenntnisse aufweist – und in der Lage ist, interdisziplinär mit Experten verschiedenster Fachrichtungen zusammenzuarbeiten. Das mag ein recht unscharfes Kriterium sein, das zudem auf viele anspruchsvolle Tätigkeiten zutrifft. Die Formulierung dieser Anforderung könnte aber helfen, die vorschnelle Einordnung von Datenschutz als rein juristische Teildisziplin zukünftig zu vermeiden.

Literatur

Bleich, H. (2011). Datenschutz im Internet: Harte Linie gegen Website-Betreiber. http://www.heise.de/newsticker/meldung/Datenschutz-im-Internet-Harte-Linie-gegen-Website-Betreiber-1193121.html (18.02.2011; zuletzt aufgerufen am 13.08.2012)

Europäische Kommission (2011). *EU-Justizkommissarin Viviane Reding: "Deutschland beim Datenschutz vorbildlich, aber Verbesserungen nötig."* http://ec.europa.eu/deutschland/press/pr_releases/9930_de.htm (04.05.2011; zuletzt aufgerufen am 13.08.2012)

Heckmann, D.-O.: *„Den Betrieben auf die Finger schauen."* http://www.dradio.de/dlf/sendungen/interview_dlf/ 539305/ (05.09.2006, zuletzt aufgerufen am 13.08.2012)

Landesbeauftragter für Datenschutz und Informationsfreiheit NRW (2012). *Schützen Sie Ihre Daten – 10 Tipps zur Datensicherheit.* https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/070328_Schuetzen_Sie_Ihre_Daten/10_Tipps_zur_Datensicherheit.pdf (28.03.2007; zuletzt aufgerufen am 13.08.2012)

Landesbeauftragter für Datenschutz und Informationsfreiheit NRW (2007). *Datensicherheit beim Telefaxverkehr.* https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/Kommunikation/Inhalt/070402_Datensicherheit_beim_Telefaxverkehr/Datensicherheit_beim_Telefaxverkehr.php (02.04.2007; zuletzt aufgerufen am 13.08.2012)

Ludwig, U., Mertin, A. & Schmid, B. (2011). *Giftige Geschäfte.* http://www.spiegel.de/spiegel/0,1518,758035,00.html (22.04.2011; zuletzt aufgerufen am 13.08.2012)

n-tv (2010). *Zahlendreher bei Hartz-IV-Gesetz – Berechnung bleibt geheim.* http://www.n-tv.de/politik/Berechnung-bleibt-geheim-article1598486.html (29.09.2010; zuletzt aufgerufen am 13.08.2012)

Reißmann, O. (2011). Interview mit Julia Schramm. http://www.spiegel.de/netzwelt/netzpolitik/internet-exhibitionisten-spackeria-privatsphaere-ist-sowas-von-eighties-a-749831.html (10.03.2011; zuletzt aufgerufen am 13.08.2012)