SSOAR

Open Access Repository
www.ssoar.info

Die Geschichte des Beschäftigtendatenschutzes - von der Unfähigkeit zum Kompromiss

Brink, Stefan

Veröffentlichungsversion / Published Version
Vortrag / lecture

Empfohlene Zitierung / Suggested Citation:
Brink, S. (2014). *Die Geschichte des Beschäftigtendatenschutzes - von der Unfähigkeit zum Kompromiss.* (Rechtspolitisches Forum, 65). Trier: Institut für Rechtspolitik an der Universität Trier. https://nbn-resolving.org/urn:nbn:de:hbz:385-8510

Nutzungsbedingungen:
Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.
Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use:
This document is made available under Deposit Licence (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual and limited right to using this document. This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.
By using this particular document, you accept the above-stated conditions of use.

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

Rechtspolitisches Forum
Legal Policy Forum

65

Stefan Brink

Die Geschichte des Beschäftigtendatenschutzes – von der Unfähigkeit zum Kompromiss

Institut für Rechtspolitik
an der Universität Trier

IRP

Rechtspolitisches Forum
65

Die Geschichte des Beschäftigtendatenschutzes – von der Unfähigkeit zum Kompromiss

von

MR Dr. Stefan Brink

Leiter Privater Datenschutz
beim Landesbeauftragten
für den Datenschutz Rheinland-Pfalz

Institut für Rechtspolitik
an der Universität Trier

IRP

Impressum

Herausgegeben von Prof. Dr. Gerhard Robbers und Prof. Dr. Thomas Raab
unter Mitarbeit von Johannes Natus, Hanna Kullmann,
Norman Koschmieder und Claudia Lehnen

Institut für Rechtspolitik an der Universität Trier · D-54286 Trier
Telefon: +49 (0)651 201-3443 · Telefax: +49 (0)651 201-3857
E-Mail: sekretariat@irp.uni-trier.de · Internet: www.irp.uni-trier.de

Die Redaktion übernimmt für unverlangt eingesandte Manuskripte keine Haftung und schickt diese nicht zurück.

Namentlich gekennzeichnete Beiträge geben nicht in jedem Fall die Meinung des Herausgebers oder der Mitarbeiter des Instituts wieder.

© Institut für Rechtspolitik an der Universität Trier, 2014
ISSN 1616-8828

Dr. Stefan Brink, Jahrgang 1966 und von Beruf Richter, promovierte bei Prof. Dr. Hans Herbert von Arnim über die Methodik der richterlichen Entscheidungsbegründung.

Er war zunächst im Wissenschaftlichen Dienst des Landtags Rheinland-Pfalz tätig, woran sich die Richtertätigkeit am Verwaltungsgericht Koblenz anschloss. Nach einer Station beim Bundesverfassungsgericht als Wissenschaftlicher Mitarbeiter im Ersten Senat bei Herrn Prof. Dr. Reinhard Gaier ist Herr Brink nun Leiter des privaten Datenschutzes beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz sowie Stellvertretender Landesbeauftragter für die Informationsfreiheit in Rheinland-Pfalz.

Herr Brink ist außerdem Lehrbeauftragter an der Deutschen Universität für Verwaltungswissenschaften in Speyer sowie an der Europa-Universität Viadrina in Frankfurt/Oder.

Schwerpunkte seiner Veröffentlichungen sind das Verfassungs- und Verwaltungsrecht, die Rechtsmethodik, sowie das Parlaments- und Datenschutzrecht.

Dieser Text ist die überarbeitete Fassung des Vortrags, den Herr Brink am 9. Dezember 2013 im Rahmen eines Rechtspolitischen Kolloquiums des Instituts für Rechtpolitik an der Universität Trier gehalten hat.

Die Geschichte des Beschäftigtendatenschutzes – von der Unfähigkeit zum Kompromiss

Die Geschichte des Beschäftigtendatenschutzes ist eine traurige Geschichte. Traurig ist sie vor allem deshalb, weil es eine ebenso langwierige wie erfolglose Geschichte ist.

Schon Norbert Blüm, Arbeitsminister in der Kohl-Ära und Erfinder der „sicheren“ Rente, hatte Ende der 80er Jahre zu Protokoll gegeben, in seiner ministerialen Schublade liege ein Gesetzentwurf zum Datenschutz für Arbeitnehmer – der bislang letzte Anlauf zur Sicherung der informationellen Selbstbestimmung der Beschäftigten scheiterte im Frühjahr dieses Jahres kläglich.[1] Der über drei Jahre beratene Gesetzentwurf der schwarz-gelben Bundesregierung[2] versandete im Innenausschuss des Bundestags.

„Warum gibt es keine Novellierung des Datenschutzrechts für Beschäftigte?“

Für diese Unfähigkeit zur Regulierung einer regulierungsbedürftigen Materie gibt es ebenso viele Gründe, wie es Betrachter dieses Scheiterns gibt. Ein Politologe wird auf den Antagonismus von Gewerkschaften und Arbeitgeberverbänden hinweisen, der sich in die politischen Parteien hinein fortsetzt; ein Verfassungsrechtler wie mein Doktorvater Hans Herbert von Arnim würde auf die Problematik der parlamentarischen Entscheidung in eigener Sache abstellen und darauf, dass jeder

---

1 Zur Geschichte des (Beschäftigten-)Datenschutzes vgl. Brink in: Wolff/Brink, Datenschutz in Bund und Ländern, 2013, Syst. C und D sowie Riesenhuber in Wolff/Brink, Datenschutz in Bund und Ländern, 2013, § 32 Rn. 1 ff.

2 BT-Drs. 17/4230 vom 15.12.2010.

Bundestagsabgeordnete selbst in eine Arbeitgeber-Arbeitnehmer-Konstellation eingeordnet sei. Und dass es eben diese Selbstbetroffenheiten seien, die Materien wie das Presserecht, die Amtshaftung oder die Versorgung von Politikern nur schwer regelbar machten. Ein Arbeitsrechtler wird das Thema Beschäftigtendatenschutz als eines von vielen ansehen, bei denen sich der Gesetzgeber – vornehm ausgedrückt – zurückhält, und etwa auf das Arbeitskampfrecht verweisen, das eben nicht durchs Parlament, sondern durch die gerichtliche Spruchpraxis reguliert ist.

Sie haben heute einen Datenschützer eingeladen – und dessen Sichtweise darf ich Ihnen nun vorstellen.

Die Frage „Warum gibt es keine Novellierung des Datenschutzrechts für Beschäftigte?“ setzt die Beantwortung einer anderen Frage voraus:

„Brauchen wir eine Novellierung des Beschäftigtendatenschutzes?“

– Und die Antwort darauf lautet: Zwei Mal ja!

Die großen Datenschutzskandale seit dem Jahre 2006 haben Verständnis und Bedeutung des Datenschutzes in der Öffentlichkeit wesentlich geprägt. Angefangen von den illegalen Daten-Screenings bei der Bahn AG, die sogar einen als unangreifbar geltenden Manager wie Hartmut Mehdorn um sein Amt brachten, über den so genannten „Lidl-Skandal“, bei dem Arbeitnehmerinnen und Arbeitnehmer bis in die Intimsphäre hinein heimlich überwacht wurden, über die Skandale bei der Deutschen Telekom, wo das Telekommunikationsgeheimnis massiv gebrochen wurde bis hin zu den Krankenrückkehrgesprächen bei Daimler.[3]

---

[3] Ein kurzer Überblick findet sich bei Riesenhuber in: Wolff/Brink, Datenschutz in Bund und Ländern, 2013, § 32 Rn. 1 ff. m.w.N.

Diese Skandale wurden nicht nur von einer sehr interessierten Öffentlichkeit wahrgenommen, sie führten auch zu relevanten Reaktionen. So hat das veränderte Kaufverhalten seiner Kunden – die Ausspähung von Mitarbeitern führte zu erheblichen Umsatzeinbußen – den Discounter Lidl dazu veranlasst, in seinen Verkaufsräumen vollständig auf Videoüberwachung zu verzichten. Die dadurch entstehenden Einbußen durch steigenden Warenschwund nimmt der Discounter offenbar gerne in Kauf, um dadurch ähnlich heftige Nachfrageeinbrüche in Zukunft vermeiden zu können.

Die Regelung, welche sich die letzte Große Koalition im Jahre 2009 in Reaktion auf diese Datenschutzskandale einigen konnte,[4] blieb jedoch rudimentär. In § 32 Abs. 1 Satz 1 des Bundesdatenschutzgesetzes wurde lediglich eine Sondernorm zur Datenverarbeitung in Beschäftigungsverhältnissen eingeführt. Danach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses nur erhoben, verarbeitet oder genutzt werden, wenn dies für das Beschäftigungsverhältnis erforderlich ist. Diese rudimentäre Regelung sollte nicht mehr als ein „Merkposten“ sein, der in der darauffolgenden Legislaturperiode durch ein echtes Beschäftigtendatenschutzgesetz ersetzt werden sollte.[5] Dazu ist es bis heute allerdings nicht gekommen.

Auf die Notwendigkeit einer Novellierung des Beschäftigtendatenschutzes weisen auch die Eingabezahlen hin, die beim Landesbeauftragten für den Datenschutz Rheinland-Pfalz seit 2008 zu verzeichnen sind. Erreichten uns im ersten Jahr unserer Zuständigkeit auch für den privaten Datenschutz gerade einmal 50 Eingaben, stieg diese Zahl bis zum Jahr 2013 auf 2.000 schriftliche und mündliche Eingaben an. Davon betrifft ca. ein Drittel Fragen des Arbeitnehmerdatenschutzes; die übrigen

---

4 BGBl. 2009 I 2814.

5 BT-Drs. 16/13657, 20.

Eingaben verteilen sich auf die Themen soziale Netzwerke / neue Medien sowie auf die „immer junge“ Thematik Videoüberwachung.[6] Auch diese Schwerpunktbildung bei den Eingaben ist aus meiner Sicht ein klarer Beleg dafür, dass das Bedürfnis nach einer gesetzlichen Regelung des Beschäftigtendatenschutzes nach wie vor sehr hoch ist.

Damit sind wir bei der Ausgangsfrage angelangt:

„Warum gibt es keine Novellierung des Datenschutzrechts für Beschäftigte?“

Meine Antwort: Weil das informationelle Selbstbestimmungsrecht (iSB) ein unverstandenes und unbefriedetes, ein **prekäres Grundrecht** ist.

Seit der Volkszählungsentscheidung des BVerfG[7] kennen wir zwar ein aus Art. 2 Abs. 1 (Recht auf freie Entfaltung der Persönlichkeit) i.V.m. Art. 1 Abs. 1 GG (Menschenwürdegarantie) abgeleitetes Datenschutzgrundrecht, dieses hat sich jedoch bis heute nicht etabliert. Es bleibt prekär i.S.v. gefährdet, instabil. Dafür gibt es Gründe.

a) Das iSB als kulturell geprägtes Recht

Das iSB basiert auf der Idee der Trennung von Öffentlichem und Privatem. Diese Idee ist aber ebenfalls instabil.

Dies lässt sich anhand zweier Bilder veranschaulichen und dokumentieren. Das eine Bild entstammt der Berliner Illustrierten Zeitung aus dem Jahre 1919 und zeigt den späteren Reichspräsidenten Friedrich Ebert, wie er sich – noch vor seiner Wahl – beim Baden im Wannsee, bekleidet nur mit einer seinerzeit

---

6 Vgl. dazu die Tätigkeitsberichte des LfDI RLP seit 2009, abrufbar unter http://www.datenschutz.rlp.de/de/ds.php?submenu=bericht.

7 BVerfGE 65, 1 ff.

gebräuchlichen Badehose, abbilden ließ.[8] Das andere zeigt den US-amerikanischen Präsidenten Obama, der im Jahre 2009 eine Bilderserie veröffentlichen ließ, die ihn – ebenfalls nur mit Badehose bekleidet – in den Wellen und am Strand von Florida zeigen.[9] Friedrich Ebert hätte diese Fotografie beinahe das Amt des Reichspräsidenten gekostet, denn viele seiner Zeitgenossen waren der Auffassung, dass eine „Respektsperson" sich in dieser Form nicht abbilden lassen dürfe. Ganz anders die Reaktionen auf den US-Präsidenten Obama im Jahre 2009, der von seinen Zeitgenossen als juvenil, aktiv und dynamisch empfunden wurde.

Kulturräume und Zeit prägen offensichtlich die Frage nach dem, was privat ist. Und: Es gibt keinen räumlich und zeitlich übergreifenden Konsens darüber, was privat ist und daher dem iSB unterfällt. Hieraus entsteht Unsicherheit und Unverständnis.

b) Das iSB als ungenutztes Recht

Die Sensibilität der Grundrechtsträger ist (wieder – nach der Generation Volkszählung) in Sachen Datenschutz recht hoch. Vor der Bundestagswahl sagten 75 % der Deutschen, dass die NSA-Affäre sie beunruhige, dass die Bundesregierung zum Schutz der Bürgerrechte gegenüber den USA tätig werden solle und dass sie die staatliche Überwachung von Telekommunikationsinhalten ablehnen; allerdings wollten nur 3 % ihre Wahlentscheidung davon abhängig machen.[10]

Dieses sog. „Datenschutz-Paradoxon" (*Jeff Jarvis*) finden wir ebenso bei der Nutzung von facebook oder Smartphones. Viele

---

8 http://upload.wikimedia.org/wikipedia/commons/8/81/Bundesarchiv_Bild_146-1987-076-13%2C_Friedrich_Ebert_u.a._beim_Baden_im_See.jpg.

9 http://kritik.blogsport.de/2009/02/19/obama-ruestet-auf-der-retter-der-welt-auf-kriegsfuss/.

10 Vgl. Bericht über eine Umfrage des Instituts für Demoskopie Allensbach für die WirtschaftsWoche, 2.11.13.

Nutzer wissen um die Gefährdung ihres iSB, entscheiden sich aber doch für eine Nutzung neuer, häufig wenig verstandener Medien.

c) Das iSB als juristisch unverstandenes Recht

Das Grundrecht auf informationelle Selbstbestimmung erweist sich aber auch als ein in nahezu jeder Hinsicht juristisch unverstandenes Recht. Dies gilt bereits für den **Gesetzgeber**: In § 1 Abs. 1 des Bundesdatenschutzgesetzes definiert er den Zweck dieses Gesetzes dahin, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird". Erstaunlicherweise kommt auch im aktuellen Bundesdatenschutzgesetz das im Jahre 1983 vom Bundesverfassungsgericht aus der Taufe gehobene informationelle Selbstbestimmungsrecht nicht vor. Stattdessen verweist der Gesetzgeber auf das ältere allgemeine Persönlichkeitsrecht (APR) und erklärt es zum Schutzgut des Datenschutzrechts.

Das ist sicher nicht ganz unrichtig. APR und iSB teilen ihren Ursprung, haben sich aber erheblich auseinanderentwickelt.[11] Das APR betrifft das Recht, eine Persönlichkeit zu sein. Nach der herrschenden Sphärentheorie schützt es die Intim- und räumliche Privatsphäre des Einzelnen, es umfasst das Recht am eigenen Wort und Bild und schützt sogar die Selbstbestimmung darüber, wie sich der Einzelne öffentlich präsentiert. Es ist als absolutes Recht i.S.v. § 823 Abs. 1 BGB anerkannt und damit wehrfähig.

Das Grundrecht auf informationelle Selbstbestimmung gewährt demgegenüber das Recht, Einfluss auf das eigene Persönlichkeits**bild** zu nehmen. Es knüpft an das 2. Biblische Gebot „Du

---

[11] Zum Verhältnis dieser Rechte vgl. Brink in: Wolff/Brink, Datenschutz in Bund und Ländern, 2013, Syst. C Verfassungsrechtliche Grundlagen, Rn. 59 ff.

sollst Dir kein Bildnis machen“ an und beruht auf der Befürchtung, dass jenes Abbild, das wir selbst und andere von uns zeichnen, die Macht hat, uns einzuschränken, uns zu beherrschen und sogar zu unterwerfen. Die technischen Innovationen wie Fotografie oder Audiografie, in heutiger Zeit die Digitalisierung unserer gesamten Lebenswelt, lassen die Gefahr, dass wir zum Sklaven unseres Persönlichkeitsprofils werden, immer realer werden. Deshalb ist das iSB vom BVerfG als „Vorfeldschutz“ präventiver Art ausgestaltet – was umgekehrt so manchen robusten Zeitgenossen zu der Einschätzung veranlasst, man solle sich mit dem Datenschutz nicht so anstellen, es sei doch noch gar nichts Schlimmes passiert.

Grob unterscheidend lässt sich sagen: Das APR schützt vor konkreten Verletzungen der Privatsphäre, das iSB schützt vor abstrakten Gefährdungen durch die Abbildung der Person. Dies drückt sich etwa dadurch aus, dass auch personenbezogene Daten mit geringem Informationsgehalt geschützt werden. In den Worten des BVerfG: Es gibt keine belanglosen Daten[12], in einer vernetzten Welt ist jedes Datum, wenn es personenbeziehbar ist, rechtlich schützenswert und geschützt. Dies greift weit über unser Verständnis des APR hinaus. Auf dieser Differenzierung beruht auch die „Grundnorm“ des Datenschutzes, § 4 Abs. 1 BDSG, der jede – auch die grundrechtlich motivierte – Verwendung personenbezogener Daten unter ein Verbot mit Erlaubnisvorbehalt stellt.

APR und iSB teilen also ihren Ursprung, haben sich aber erheblich auseinanderentwickelt. Dass selbst das BDSG dies nicht zur Kenntnis nimmt, ist – gelinde gesagt – ein schlechter Witz.

---

12 BVerfGE 65, 1 (45); 120, 378 (399).

Als juristisch unverstandenes Recht erweist sich das informationelle Selbstbestimmungsrecht auch dann, wenn man sich anschaut, wie die Beratung zum Beschäftigtendatenschutzgesetz-Entwurf der Bundesregierung[13] in den Jahren 2010 bis 2013 vonstatten ging. Ein besonders gutes Beispiel ist da der § 32d des Gesetzentwurfs der Bundesregierung, der sich mit der Datenverarbeitung im Beschäftigungsverhältnis befasste. Nach § 32d Abs. 3 des Gesetzentwurfs sollte der Arbeitgeber zur Aufdeckung von Strafdaten durch Beschäftigte einen automatisierten Abgleich „bereits vorhandener Beschäftigtendaten" durchführen dürfen. Diese als „Eh-da-Prinzip" verspottete Regelung unternahm nichts anderes als eine Aufhebung des fundamentalen Zweckbindungsgrundsatzes im § 4 Abs. 2 und 3 BDSG. Ausdruck der informationellen Selbstbestimmung ist es gerade, den Verwendungskontext von personenbezogenen Daten als Grundrechtsträger selbst setzen und auf der Einhaltung dieser Zweckbindung bestehen zu dürfen. Dass der Gesetzgeber offensichtlich beabsichtigt hat, die bislang gesetzlich gänzlich unbekannte Kategorie „bereits vorhandener Daten" einzuführen, belegt, wie wenig gefestigt die Vorstellung von der informationellen Selbstbestimmung sogar beim Gesetzgeber und dem ihm zuarbeitenden Bundesministerium des Innern ist. Dasselbe Unverständnis zeigt sich in „schöner" Regelmäßigkeit bei der politischen Diskussion über die Zweckentfremdung von Abrechnungsdaten für die Lkw-Maut. Obwohl der damalige Bundesinnenminister Schäuble gegenüber dem Deutschen Bundestag unzweifelhaft und nachdrücklich bekräftigt hatte, dass diese Abrechnungsdaten niemals für andere als Abrechnungszwecke eingesetzt würden, flammt die Diskussion darüber, ob man die Mautdaten nicht ebenso für die Verfolgung (spektakulärer) Straftaten verwenden sollte, da sie doch „ohnehin bereits da seien", immer wieder neu auf.

---

13 BT-Drs. 17/4230 vom 15.12.2010.

Mit seinem Unverständnis für das informationelle Selbstbestimmungsrecht steht der Gesetzgeber aber keinesfalls alleine da. Auch die **Fachgerichte** ignorieren regelmäßig Existenz, Inhalt und Reichweite der informationellen Selbstbestimmung. Dies tut etwas das Bundesarbeitsgericht, wenn es in ständiger Rechtsprechung die eindeutige, in § 6b Abs. 2 BDSG niedergelegte gesetzliche Hinweispflicht für jede Form der Videoüberwachung im öffentlichen Raum als „bloße Ordnungsvorschrift" wertet und die doch offenkundig gesetzeswidrige heimliche Videoüberwachung in Ausnahmefällen für statthaft hält.[14]

Auch die bekannte „Spick-mich-Entscheidung" des Bundesgerichtshofs[15] lässt sich in die Kategorie „unverstandenes Grundrecht" mühelos einordnen. Hier musste sich das Bundesgericht mit der schwierigen Frage auseinandersetzen, ob die Betreiber von Lehrer-Bewertungsportalen im Internet bestimmte Informationspflichten gegenüber den betroffenen Lehrerinnen und Lehrern haben und ob ihnen insbesondere eine Prüfpflicht bezüglich der Besucher ihrer Portalseiten von Gesetzes wegen auferlegt ist. In genau diesem Sinne lässt sich § 29 Abs. 2 des Bundesdatenschutzgesetzes verstehen, der einem Zugriffswilligen nur unter der Voraussetzung eines (geprüften) berechtigten Interesses Zugang zu einem solchen Portal eröffnet. Der Bundesgerichtshof hat eine solche Prüfpflicht contra legem[16] nicht nur verneint – dies wäre sicherlich das Ende solcher Bewertungsportale gewesen, da die Betreiber den Aufwand einer solchen Einzelfallprüfung wohl kaum hätten bewältigen wollen –, der BGH hat die Vorschrift schlicht mit der Begründung unangewendet gelassen, es handele sich bei § 29 BDSG um eine

---

14 BGH NZA 2003, 1193 m.w.N.

15 BGH, Urteil vom 23.06.2009 – VI ZR 196/08 – NJW 2009, 2888.

16 BGH, Urteil vom 23.06.2009 – VI ZR 196/08 – Rn. 42.

Rechtsregelung, die aus „Vor-Internet“-Zeiten stamme und die deshalb auf Internet-Bewertungsportale nicht passe.[17]

Damit hat es – deklariert als „nicht wortgetreue“ „verfassungskonforme Auslegung“, also contra legem – zugleich seine in Artikel 100 Abs. 1 Grundgesetz niedergelegte Vorlagepflicht an das Bundesverfassungsgericht verletzt, wonach alleine das Verfassungsgericht befugt ist, nachkonstitutionelles formelles Recht zu verwerfen bzw. außer Anwendung zu lassen.

Auch der **Bundesfinanzhof** fremdelt mit dem „schwierigen“ Grundrecht auf informationelle Selbstbestimmung, wenn er etwa im Rahmen von Zollverfahren die Durchführung von Mitarbeiter-Screenings gegen nationale und internationale Terrorlisten ohne jede gesetzliche Grundlage toleriert[18] – und Arbeitgeber, die das iSB ihrer Mitarbeiter und Kunden respektvoll behandeln möchten, frustriert.[19] Offenbar heiligt hier der gute Zweck Terrorismusbekämpfung jeden Eingriff in Grundrechte.

Und die **Rechtswissenschaft**?

Auch die wissenschaftliche Durchdringung der Materie Datenschutz ist ausbaufähig; hier lässt sich noch mit überschaubarem Aufwand Mehrwert erzeugen. Zwei klare Gedanken und man findet sich an der „Spitze der wissenschaftlichen Bewegung“.

1. Gedanke: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit befasst sich mit dem Datenschutz einerseits und der Informationsfreiheit andererseits, also mit zwei

---

17 BGH, Urteil vom 23.06.2009 – VI ZR 196/08 – Rn. 42: „Hierfür ist zu bedenken, dass ein durch Portalbetreiber organisierter Informationsaustausch im Internet weder technisch möglich war noch dergleichen für denkbar gehalten wurde, als § 29 BDSG am 1. Juni 1991 Eingang in das Bundesdatenschutzgesetz gefunden hat.“

18 BFH 7. Senat, Urteil vom 19.06.2012 – VII R 43/11 – ZD 2013, 129 mit Anmerkung von Brink jurisPR-ArbR 45/2012 Anm. 3.

19 Vgl. Brink, jurisPR-ArbR 45/2012 Anm. 3.

prinzipiell unvereinbaren Materien: Beim Datenschutz erklären wir den Behörden, dass sie Daten nicht herausgeben dürfen, und bei der Informationsfreiheit erklären wir ihnen, dass sie Daten herausgeben müssen. Und zwar an jedermann, ohne Prüfung eines berechtigten Interesses. Wer auch immer aus welchem Grund auch immer Einblick in Unterlagen nehmen möchte, die einer Behörde vorliegen, der kann und darf dies nach dem Landesinformationsfreiheitsgesetz LIFG tun. Manche Behörden verzweifeln gerade an dieser Aufgabe; Ministerpräsidentin Malu Dreyer hat die transparente und auskunftsfreudige Verwaltung aber gerade zu einem Schwerpunkt ihrer Regierungszeit erklärt. Ist es also eine gute Idee, eine Behörde für Datenschutz **und** Informationsfreiheit zu schaffen?

2. Gedanke: Auf Georg Jellineks Schrift „System der subjektiven öffentlichen Rechte“ aus dem Jahre 1892 geht die sog. Statuslehre zurück. Danach lassen sich verschiedene Grundrechtsdimensionen unterscheiden, nämlich abwehrrechtliche (status negativus), anspruchsrechtliche (status positivus) und teilhaberechtliche (status activus). Das iSB lässt sich als Recht verstehen, Informationsbegehren des Staats negierend abzuwehren. Der Anspruch aus dem Informationsfreiheitsgesetz gegen staatliche Stellen lässt sich dem aktiven Status (als Anspruch) zuordnen; er dient der Gewinnung von Wissen, um staatliche Stellen besser kontrollieren und selbst am öffentlichen demokratischen Diskurs teilnehmen zu können (vgl. § 1 Abs. 1 LIFG RLP, status activus). So gesehen gibt es nur ein Grundrecht mit dem Namen Informationsfreiheit, dessen Ausprägungen durch das BDSG bzw. die LDSG einerseits und die Informationsfreiheitsgesetze andererseits erfolgen.

Wenn das BVerfG 1983 also vom iSB sprach, meinte es eigentlich: Informationsfreiheit. Datenschutz ist Informationsfreiheit! Informationsfreiheit betrifft danach alle Informationsbeziehungen zwischen Staat und Bürger, mittelbar – vermittelt nämlich

durch Gesetze, die der staatlichen Pflicht zum Schutz der Grundrechte genügen, wie etwa der dritte Abschnitt des BDSG – auch diejenigen zwischen Bürgern. Und deshalb sind auch beide Aspekte beim LfDI gut aufgehoben. Zwei Gedanken, eine Dissertation.

Auch bei ganz praktischen Fragen des Datenschutzes kann die Rechtswissenschaft wenig Orientierendes anbieten, sie stellt allenfalls „Streitstände“ zur Verfügung. Schauen wir auf § 4 Abs. 1 BDSG, die zentrale Norm des BDSG. Danach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Im Wege der Einwilligung verfügt der Grundrechtsberechtigte also über das Schutzgut der informationellen Selbstbestimmung, nämlich seine personenbezogenen Daten. Nach § 4a BDSG sind an eine solche Einwilligung einige Bedingungen geknüpft. Wirksam ist sie nach dieser Vorschrift nämlich nur dann, wenn sie freiwillig, also ohne Zwang und mit der Möglichkeit alternativer Verhaltensweisen abgegeben wurde.[20] Auf die Freiwilligkeit seiner Einwilligungserklärung ist der Betroffene hinzuweisen, er kann diese Erklärung sowohl beschränken als auch mit Blick auf die Zukunft widerrufen. Aus § 4a BDSG ergibt sich ferner, dass diese Einwilligung „informiert“, also in Kenntnis der Zwecke der Datenverarbeitung und der konkreten Gestaltung der Datenverwendung abgegeben werden muss.[21] Sie ist in der Regel schriftlich und getrennt von anderen Willenserklärungen abzugeben.

---

20 Dazu ausführlich Kühling in: Wolff/Brink, Datenschutz in Bund und Ländern, 2013, § 4a Rn. 35 ff.

21 Vgl. Kühling in: Wolff/Brink, Datenschutz in Bund und Ländern, 2013, § 4a Rn. 43.

Bezogen auf die uns hier interessierende Frage des Beschäftigtendatenschutzes ergeben sich daraus eine Reihe von Folgefragen: Ist die Einwilligung im Arbeitsverhältnis wirksam? Sind Betriebsvereinbarungen eine wirksame Grundlage für Datenverwendungen? Dürfen Betriebsvereinbarungen von Vorgaben des BDSG abweichen? Gibt es einen „betrieblichen Datenschutzstandard“? Die Antworten der Rechtswissenschaft hierzu fallen höchst unterschiedlich aus, eine einheitliche Rechtsauffassung hat sich nicht herausgebildet.[22] Auch deshalb brauchen wir ein Gesetz zur Regelung des Beschäftigtendatenschutzes.

Soweit zu den staatlichen Stellen.

Was machen nun aber die **Bürger**?

Die Nutzung ihrer Datenschutzrechte durch die Bürgerinnen und Bürger ist nach wie vor zurückhaltend. Von den gesetzlichen Rechten auf Auskunft (§ 34 BDSG), Löschung und Berichtigung personenbezogener Daten (§ 35 BDSG) wird nur höchst zurückhaltend Gebrauch gemacht. Die Zahl der Petitionen von Arbeitnehmern an den Landesbeauftragten für Datenschutz in Rheinland-Pfalz ist zwar enorm gestiegen, absolut betrachtet handelt es sich jedoch noch keineswegs um eine breite Bewegung. Allerdings haben immer mehr **Betriebsräte** die Thematik Arbeitsnehmerdatenschutz inzwischen für sich entdeckt und nehmen die Beratungsangebote des Landesbeauftragten, insbesondere im Rahmen von Schulungsmaßnahmen, immer häufiger an.

Die Haltung vieler **Arbeitgeber** zum Thema Datenschutz lässt sich ihren Homepages entnehmen. Dort steht in schöner Regelmäßigkeit geschrieben: „Der Datenschutz genießt in unserem Unternehmen schon immer einen hohen Stellenwert, und

---

[22] Zum Streitstand vgl. Riesenhuber in: Wolff/Brink, Datenschutz in Bund und Ländern, 2013, § 32 Rn. 37 ff.

zwar nicht etwa aufgrund des öffentlichen Drucks und des Medieninteresses an dem Thema, sondern aus Überzeugung und Respekt vor den Rechten unserer Mitarbeiter und Kunden.“ Aus der Prüfpraxis des LfDI wissen wir, dass dieser Erklärung regelmäßig die Einschränkung beigefügt wird „… solange dadurch keine Kosten verursacht, unsere Verfahrensstandards nicht angetastet und unsere Geschäftstätigkeit nicht eingeschränkt wird.“

Das Hauptargument gegen den Datenschutz ist nach wie vor – und zwar sowohl bei Privaten, als auch bei staatlichen Überwachungsstellen: Wer nichts zu verbergen hat, der muss sich vor Überwachung auch nicht fürchten. Dieses ebenso wohlfeile wie unterkomplexe Argument verleugnet, dass jeder von uns etwas zu verbergen hat, weil er eine vielschichtige und differenzierte Persönlichkeit ist. Dieses Argument übersieht, dass es niemanden etwas angeht, dass ich nichts zu verbergen habe. Und es übersieht die einfachste Regel des „Informations-Managements“[23]: Sagen Sie alles Ihrer Mutter, was Sie auch Ihrer Frau sagen? Und umgekehrt? Und: Sind Sie deshalb unehrlich?

---

[23] Vgl. Brink in: Wolff/Brink, Datenschutz in Bund und Ländern, 2013, Syst. C Verfassungsrechtliche Grundlagen, Rn. 9.

Fazit

Es gibt **keinen gesellschaftlichen Konsens** zur Bedeutung des iSB, zu seinem Wert, zu seinem Gewicht bei der Abwägung mit gegenläufigen Werten wie wirtschaftlicher Effizienz (Stichwort Einsatz von Ortungssystemen zur Koordination des Einsatzes von Arbeitnehmern), wie unternehmerischer Selbstbestimmung (Stichwort: Compliance, also insbesondere dem Schutz des Arbeitgebers vor Schädigung durch den Arbeitnehmer), des relativen Wertes von staatlichen Überwachungs- und Verfolgungsinteressen (Stichwort Mautdaten zur Strafverfolgung) und des Wertes internationaler Beziehungen (Stichwort NSA und No-Spy-Abkommen). Was es gibt ist – ich möchte sagen: leider – einen Bundesinnenminister, der von einem „Supergrundrecht auf Sicherheit“ spricht und sich gleichzeitig wegen seiner Ressortzuständigkeit für den Datenschutz „Oberster Datenschützer Deutschlands“ tituliert. Von einem Konsens sind wir meilenweit entfernt.

Ohne diesen Konsens aber wird jede Gesetzgebung zum Datenschutz ein unberechenbares Unterfangen. Dies gilt für die internationale Ebene, also etwa für die Frage der datenschutzrechtlichen Ergänzung von Welt-Handelsabkommen in besonders starkem Maße, aber ebenso für supranationale Vereinbarungen wie eine EU-Datenschutzgrundverordnung oder eben für ein nationales Beschäftigtendatenschutzgesetz.

Der aktuelle Koalitionsvertrag von Schwarz-Rot[24] befasst sich auch mit dem Beschäftigtendatenschutz. Dort steht geschrieben:

---

[24] Abrufbar unter http://www.tagesschau.de/inland/koalitionsvertrag136.pdf.

„Beschäftigtendatenschutz gesetzlich regeln

Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen.“

Keine inhaltlichen Vorgaben also, auf die man sich verständigt hätte, keine klaren zeitlichen Vorgaben. Raten Sie mal, was am Ende dabei herauskommen wird.

Aber ich sagte es ja schon: Das ist eine traurige Geschichte.

Das Institut für Rechtspolitik an der Universität Trier hat die wissenschaftliche Forschung und Beratung auf Gebieten der Rechtspolitik sowie die systematische Erfassung wesentlicher rechtspolitischer Themen im In- und Ausland zur Aufgabe. Es wurde im Januar 2000 gegründet.

In der Schriftenreihe Rechtspolitisches Forum veröffentlicht das Institut für Rechtspolitik Ansätze und Ergebnisse national wie international orientierter rechtspolitischer Forschung, die als Quelle für weitere Anregungen und Entwicklungen auf diesem Gebiet dienen mögen.

Das Rechtspolitische Forum erscheint mehrmals jährlich. Publikationen dieser Reihe können gegen Entrichtung einer Schutzgebühr beim Institut für Rechtspolitik erworben werden.

Eine Übersicht aller Publikationen des Instituts für Rechtspolitik steht im Internet unter www.irp.uni-trier.de zur Verfügung.

Institut für Rechtspolitik
an der Universität Trier

D-54286 Trier
Telefon: +49 (0)651 201-3443
Telefax: +49 (0)651 201-3857
E-Mail: sekretariat@irp.uni-trier.de
Internet: www.irp.uni-trier.de

Die Geschichte des Beschäftigtendatenschutzes – von der Unfähigkeit zum Kompromiss.

In der Folge der großen Datenschutzskandale seit dem Jahre 2006, darunter die illegalen Daten-Screenings bei der Bahn AG, oder auch der „Lidl-Skandal", bei dem Arbeitnehmer und Arbeitnehmerinnen bis in die Intimsphäre heimlich überwacht worden sind, ist das Thema Datenschutz stark in den Fokus der Öffentlichkeit gerückt.

Schon seit den 80er Jahren liegt ein Gesetzentwurf zum Datenschutz für Arbeitnehmer in den ministerialen Schubladen, aber auch der letzte Anlauf zur gesetzlichen Sicherung der informationellen Selbstbestimmung der Beschäftigten scheiterte im Frühjahr des Jahres 2013.

Das große Bedürfnis einer gesetzlichen Ausgestaltung dieser Materie besteht nach wie vor. Dies kann jedoch nur gelingen, wenn es endlich zu einem gesellschaftlichen Konsens, vor allem auch international, über das Gewicht gegenläufiger Werte wie wirtschaftlicher Effizienz, dem Schutz des Arbeitgebers vor Schädigung durch den Arbeitnehmer, sowie dem staatlichen Verfolgungsinteresse kommt. Vor allem aber bedarf es auch einer erhöhten Sensibilität für datenschutzrechtliche Probleme, sowohl in der Bevölkerung, als auch bei Verwaltung und Justiz.

Institut für Rechtspolitik an der
Universität Trier

ISSN 1616-8828