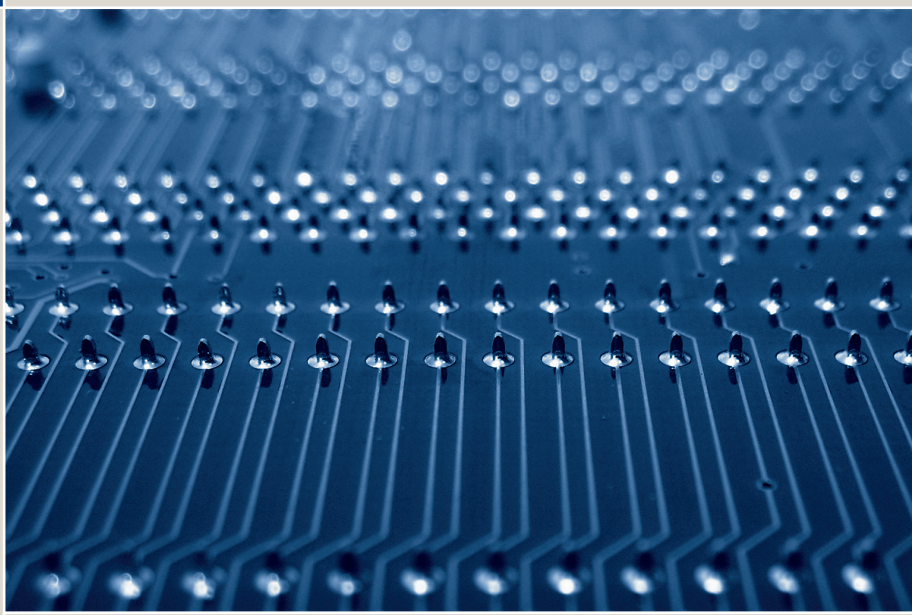
27

Recht und Neue Medien

LEIBLE · KUTSCHKE (Hrsg.)



Der Schutz der Persönlichkeit im Internet

BOORBERG

Der Schutz der Persönlichkeit im Internet

Herausgegeben von
Prof. Dr. Stefan Leible
und
Torsten Kutschke

BOORBERG

Bibliografische Information der Deutschen Nationalbibliothek | Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über www.dnb.de abrufbar.

ISBN 978-3-415-04915-4 E-ISBN 978-3-415-04993-2

Satz: Dörr + Schiller GmbH, Curiestraße 4, 70563 Stuttgart | Druck und Bindung: Gulde Druck, Hechinger Straße 264, 72072 Tübingen

Richard Boorberg Verlag GmbH & Co KG | Scharrstraße 2 | 70563 Stuttgart
Stuttgart | München | Hannover | Berlin | Weimar | Dresden
www.boorberg.de

Vorwort

Der im Frühjahr 2000 gegründete Bayreuther Arbeitskreis für Informationstechnologie – Neue Medien – Recht e.V., kurz @kit, hat sich zum Ziel gesetzt, das Recht der neuen Informationsmedien näher auszuleuchten und hierbei gewonnene Erkenntnisse in praxistauglicher Form der interessierten Öffentlichkeit zu vermitteln. Besonderer Wert wird dabei auf einen interdisziplinären Ansatz gelegt. Im Arbeitskreis wirken daher nicht nur Vertreter der verschiedenen juristischen Fachrichtungen, sondern auch Betriebs- und Volkswirte, Ingenieure, Techniker u. a. mit. Durch die enge Anbindung des Arbeitskreises an die Universität Bayreuth werden außerdem die ständige wissenschaftliche Begleitung aller in Angriff genommenen Projekte sowie ein reger Know-how-Transfer zwischen Wissenschaft und Praxis sichergestellt. Der Arbeitskreis ist freilich keine auf Bayreuth begrenzte lokale Veranstaltung. @kit steht vielmehr allen am Informationsrecht Interessierten aus dem gesamten Bundesgebiet und darüber hinaus offen. Weitere Mitstreiter sind herzlich willkommen! Nähere Informationen finden sich unter www.ak-it-recht.de.

Dieser Band präsentiert die Schriftfassung aller Vorträge, die während des 12. @kit-Kongresses, der zugleich das 2. Forum „Kommunikation & Recht“ war und am 21./22. Juni 2012 in Hamburg unter dem Generalthema „Der Schutz der Persönlichkeit im Internet“ stattfand, gehalten wurden.

Fester Bestandteil eines jeden @kit-Kongresses ist die Podiumsdiskussion, die sich heuer mit der Frage „Datensammelwut vs. Datenschutz – Brauchen wir eine neue Datenschutzpolitik?“ beschäftigte. Sie stand unter der Leitung von Herrn Rechtsanwalt *Martin W. Huff*, Journalist und Lehrbeauftragter für Medienrecht, und war – wie immer – hochkarätig besetzt:

- MdB Dr. *Konstantin von Notz*, Bündnis 90/DIE GRÜNEN, Berlin
- RA Dr. *Gunnar Bender,* Direktor Policy Facebook Deutschland GmbH, Berlin
- Dr. *Arnd Haller*, Leiter Recht Google Germany GmbH, Hamburg
- *Lorenz Matzat*, Digitale Gesellschaft e.V./OpenDataCity, Berlin

Die im Verlauf der äußerst spannenden und lebhaften Diskussion von den auf dem Podium anwesenden Teilnehmern vertretenen Standpunkte werden in diesem Tagungsband dokumentiert.

Eine Tagung wie diese bedarf der Unterstützung durch Sponsoren. Zu danken haben wir unseren Hauptsponsoren, allen voran der united domains

AG, Starnberg, und weiterhin der Firma DATSEC ® Data Security e. K., Jena. Dank gebührt darüber hinaus unseren weiteren Unterstützern, insbesondere den Kanzleien JBB Rechtsanwälte, Norton Rose, Härting Rechtsanwälte und BBS Rechtsanwälte. BBS Rechtsanwälte standen uns auch bei der Organisation des Kongresses in Hamburg hilfreich zur Seite. Wir danken außerdem herzlich der Gruner + Jahr AG & Co. KG, in deren wunderschönen Räumen am Baumwall wir tagen durften. Unser Dank gilt schließlich auch dem Kompetenzzentrum für den elektronischen Geschäftsverkehr in Ober- und Mittelfranken (KEGOM), der Arbeitsgemeinschaft Informationstechnologie im Deutschen Anwaltverein (DAV IT-Recht/davit.de) sowie dem Verlag Richard Boorberg für ihre sonstigen Hilfen bei der Vorbereitung und Durchführung des Kongresses.

Wir danken weiterhin Frau *Kirstin Freitag*, die die Manuskripte der Referenten betreut und in einen druckfertigen Zustand gebracht hat. Zu Dank verpflichtet sind wir daneben den Mitarbeitern des Lehrstuhls Prof. Dr. Stefan Leible sowie der Kanzleien GRUENDEL (Jena) und Rosenschon Sperber Grimme Henker (Bayreuth) und weiterhin dem Team vom Deutschen Fachverlag GmbH (Frankfurt a. M.), die bei der Vorbereitung des Kongresses mitgewirkt und so zu seinem Gelingen beigetragen haben.

Abschließend ist noch darauf hinzuweisen, dass der 13. @kit-Kongress bzw. das 3. Forum „Kommunikation & Recht“ am 13./14. im Juni 2013 in Berlin stattfinden wird.

Bayreuth und Frankfurt a. M., im September 2012 Die Herausgeber

Inhaltsverzeichnis

Der Schutz der Persönlichkeit im Internet

Hans-Heinrich von Knobloch[1]

Inhaltsverzeichnis

Die Aktivitäten von globalen Internetunternehmen wie Facebook oder Google werden in der breiten Öffentlichkeit, aber auch in Fachkreisen, überwiegend als eine Debatte über den Datenschutz wahrgenommen. Unterpunkte dieser Debatte sind

– die sich verschiebenden Grenzen zwischen Privatheit und Öffentlichkeit,
– die Kommerzialisierung der Privatsphäre und *last but not least*
– die Notwendigkeit einer Strategie zum Schutz der Privatheit.

Am Ende geht es in der Debatte in der Regel um Risiken. Das Datenschutzrecht soll diese Risiken bereits im Vorfeld ausschließen oder zumindest minimieren.

Das Internet ist nicht nur ein datenschutzrechtliches, noch nicht einmal nur ein rechtliches, sondern auch und vor allem ein gesellschaftliches Phänomen mit vielen unterschiedlichen Facetten.

Was bedeutet es dann aber, wenn diese unterschiedlichen Facetten in Deutschland und Europa vor allem unter dem Gesichtspunkt des Datenschutzrechts diskutiert werden? Liegt hierin nicht eine unzulässige Verkürzung der Diskussion? Oder umgekehrt formuliert: Wird hier das Datenschutzrecht nicht überschätzt, überstrapaziert und im Ergebnis auch überfordert?

---

1 Der Beitrag beruht auf einer Rede von Frau Staatssekretärin Rogall-Grothe, BMI, gehalten an der Deutschen Universität für Verwaltungswissenschaften Speyer bei der Tagung „Facebook, Google und Co." am 26. April 2012.

Es handelt sich hierbei nicht nur um theoretische Fragen. Die Debatte um die Reform des Europäischen Datenschutzrechts ist derzeit in vollem Gange. Die Europäische Kommission hat am 25. Januar 2012 ihre Vorschläge für zwei neue Rechtsakte vorgestellt, darunter einen Vorschlag für eine Datenschutz-Grundverordnung zur Ablösung der geltenden EG-Datenschutzrichtlinie 95/46/EG. Die Beratungen hierzu in der Ratsarbeitsgruppe haben begonnen. Inhalt und Reichweite der Europäischen Reform werden maßgeblich davon geprägt sein, was nach Ansicht der Europäischen Kommission, des Europäischen Parlaments und der Mitgliedsstaaten im Rat der Europäischen Union dem Datenschutzrecht unterfällt – und was nicht.

I. Das Internet als datenschutzrechtliche Herausforderung

Wir sollten uns stets die Lebenswirklichkeit und den Regelungsgegenstand vor Augen halten. Die Lebenswirklichkeit und Sachverhalte, an die wir die rechtlichen Maßstäbe des Datenschutzrechts anlegen, werden immer breiter und vielfältiger. Das Internet dringt in alle Lebensbereiche vor. Es steuert unsere Autos und regelt unseren Stromverbrauch. In der Landwirtschaft lassen sich dank GPS und Internet Felder punktgenau und umweltgerecht düngen. Das Wichtigste aber ist, dass sich unsere gesamte Kommunikation zunehmend ins Internet verlagert. Das Datenschutzrecht soll Antworten auf Inhalt und Grenzen von Kommunikations- und Informationsvorgängen geben.

Kann es das eigentlich? Das Datenschutzrecht dient dem Schutz der Persönlichkeitsrechte. So, wie wir das Datenschutzrecht konzipiert haben, fragen wir aber nicht danach, ob bzw. wie stark Persönlichkeitsrechte tatsächlich beeinträchtigt sind. Wir setzen vorher an und sagen: „Es gibt kein belangloses Datum. Jede Datenverarbeitung kann gefährlich sein. Deshalb müssen wir jeden einzelnen Schritt der Datenverarbeitung regeln. Und alles, was nicht geregelt und für zulässig erklärt wurde, ist verboten“. Bei diesem Konzept rückt die Frage, wie sich eigentlich die konkrete Datenverarbeitung auf die Persönlichkeitsrechte auswirkt, zunächst völlig aus dem Blickfeld. Erst am Ende der Einzelfallprüfung – bei der Verhältnismäßigkeit – taucht sie wieder auf. Die Abbildung einer Häuserfassade bei Google Street View und die kommerzielle und massenhafte Profilbildung durch Datenhändler – regulatorisch stellen wir erst einmal alles auf eine Stufe. Werden wir mit diesem Ansatz den tatsächlichen Risiken eigentlich gerecht? Und verbauen wir

uns auf der anderen Seite nicht Chancen und Freiheiten in den Fällen, wo die Gefahren für die Persönlichkeitsrechte eher gering sind?

Soziale Netzwerke und das Internet werfen komplexe und teilweise völlig neue datenschutzrechtliche Fragen auf. Die Reform des Datenschutzrechts stellt eines der wichtigsten und zugleich herausforderndsten Themen der Informationsgesellschaft dar. Selbst wenn man für eine differenzierte Herangehensweise plädiert und vor einer „Überreformierung" warnt, verbleiben immer noch große Herausforderungen: Das geltende Datenschutzrecht stammt aus der Zeit vor dem Internet. Seine Verfasser gingen von gänzlich anderen Voraussetzungen aus, als wir sie heute haben. Die private Nutzung von Sozialen Netzwerken lässt sich nicht mit der staatlichen Volkszählung von einst vergleichen. Dasselbe gilt für andere Alltäglichkeiten des Internets, wie Mails, Twitter, Blogs und die zahlreichen mobilen Anwendungen, von denen wir mit unseren Smartphones Gebrauch machen.

Das Internet führt dazu, dass dem Datenschutzrecht im privaten Bereich bzw. dem Bereich der Wirtschaft eine viel stärkere Bedeutung zukommt als früher. Stand zunächst eher das Verhältnis zwischen Staat und Bürger im Mittelpunkt der datenschutzrechtlichen Regelungen, rückt mit dem Internet die Beziehung zwischen Bürger und Bürger bzw. zwischen Bürger und Wirtschaft in den Fokus.

Diese tatsächliche Entwicklung zwingt zu einer Neubeurteilung des Datenschutzrechts und zu einer stärkeren Trennung zwischen dem öffentlichen und nichtöffentlichen Bereich. Im öffentlichen Bereich – im Verhältnis Staat-Bürger – hat sich die Systematik des Datenschutzrechts mit seinem Verbot mit Erlaubnisvorbehalt bewährt. Der Staat ist durch die Grundrechte verpflichtet. Sein Handeln bedarf der Rechtfertigung. Für den nichtöffentlichen Bereich entsteht die Frage nach neuen Wegen. Das Nachdenken darüber, wie wir dort stärker eingreifen und schützen können, wo größere Gefahren für die Persönlichkeitsrechte lauern als bei einer provokant – eigentlich „belanglosen Datenverarbeitung"?

Ein modernes Datenschutzrecht darf sich den Möglichkeiten und Chancen des Internets nicht verschließen. Ebenso muss es auf die neuen Herausforderungen und Gefahren angemessen reagieren. Bei den anstehenden Reformen wird es daher auch und vor allem darum gehen, das Datenschutzrecht dem Internetzeitalter anzupassen. Mit der jetzigen Systematik droht die Kapitulation des Datenschutzrechts vor der Komplexität des Internets. Statt alles allumfassend präventiv zu regeln, sollten präventive und repressive Maßnahmen im privaten Datenschutzrecht nach Risiken gestaffelt werden.

II. Keine Überstrapazierung des Datenschutzrechts/ der rechtsvergleichende Blick

„Die Dosis macht das Gift". Diese Feststellung von Paracelsus trifft nicht nur auf die Medizin zu. Schutz darf nicht zum Selbstzweck werden, Hilfe nicht in einen pathologischen Komplex umschlagen.

Es besteht die Gefahr, dass das Bemühen um einen guten Datenschutz übertrieben und das Datenschutzrecht mit Themen überfrachtet wird, die es eigentlich nicht bewältigen kann. Es lohnt sich, auf das Schutzgut des Datenschutzrechts zu schauen. Nach § 1 des Bundesdatenschutzgesetzes und Art. 1 der geltenden EG-Datenschutzrichtlinie 95/46/EG ist dies das Persönlichkeitsrecht respektive die Privatsphäre. In der englischen Textfassung wird beides mit „Privacy" übersetzt.

Der Begriff „Privacy" führt ins amerikanische Datenschutzrecht. Ein rechtsvergleichender Blick hilft, das eigene Datenschutzrecht besser zu verstehen.

(The Right to) Privacy hat in den USA eine lange Tradition, die sich aus dem 4. Zusatzartikel der Verfassung ableitet. Bereits im Jahr 1890 definierten der spätere Richter *Louis Brandeis* gemeinsam mit dem Schriftsteller und Rechtsanwalt *Samuel D. Warren* das Recht auf Privacy als „*right to be let alone*" – also als das „Recht, in Ruhe gelassen zu werden".

Anfang der 1960er-Jahre bestimmte das Recht auf Privacy dann die beginnende Debatte um das amerikanische Datenschutzrecht: Die Regierung unter John F. Kennedy hatte geplant, ein Nationales Datenzentrum zur Verbesserung des staatlichen Informationswesens einzurichten, in dem Daten aller US-Bürger registriert werden sollten. Der Kongress betrachtete dieses Vorhaben jedoch als einen Eingriff in das verfassungsrechtlich gewährleistete „*right to be let alone*" und ließ es deshalb scheitern. Forderungen nach einer gesetzlichen Grundlage für die Verarbeitung personenbezogener Daten wurden laut. Ergebnis war die Verabschiedung des sogenannten *Privacy Act* im Jahre 1974, der die amerikanischen Bundesbehörden zur Einhaltung datenschutzrechtlicher Prinzipien verpflichtete.

Über die in den USA geführte Debatte wurde auch in Deutschland und Europa berichtet. Von einer unmittelbaren Übersetzung des Begriffs „Privacy" wurde aber bewusst abgesehen und stattdessen in der Wissenschaft das Wort „Datenschutz" geschaffen, das inzwischen nicht nur in Deutschland, sondern auch international gebräuchlich ist.

Schon damals wurde allerdings erkannt und auch kritisiert, dass der Begriff „Datenschutz" in die Irre führt: Denn es ist gerade nicht das Anliegen des

Datenschutzes, Daten zu schützen. Es geht darum, den Menschen zu schützen. Deutlich wird dies in der – allerdings erst im Jahre 1990 in das Gesetz aufgenommenen – Formulierung zu Zweck und Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG). Dort heißt es (§ 1 BDSG):

> *„Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird".*

Eine ähnliche Regelung lässt sich – wie bereits erwähnt – in der geltenden Datenschutzrichtlinie 95/46/EG finden. Dort heißt es ganz am Anfang (Art. 1 Abs. 1), dass es um den Schutz der Privatsphäre natürlicher Personen geht.

III. Datenschutz als Persönlichkeitsschutz

Der Mensch, nicht seine Daten, steht also im Mittelpunkt.

Es wäre konsequent, wenn das Datenschutzrecht bei der Frage ansetzte, ob und inwieweit das Persönlichkeitsrecht beeinträchtigt ist. Stattdessen wird der Schutz personenbezogener Daten an sich zum Ziel erklärt. Regelungstechnisch wird der Vorgang der Datenverarbeitung in den Mittelpunkt gerückt. Regelungsgegenstand ist das einzelne Datum, seine Erhebung, seine Speicherung, seine Übermittlung usw. Das bedeutet im Ergebnis nichts anderes, als dass der inhaltliche Gehalt des Privacy-Begriffs zwar Einzug in die Zielbestimmungen unserer Datenschutzgesetze gehalten hat. Die datenschutzrechtlichen Regelungen aber setzen diesen Gedankengang nicht fort, sondern betreiben „Daten-Schutz" im wörtlichen Sinne: Sie schützen das einzelne Datum, nicht den Menschen. Wenn man so will, verliert das Datenschutzrecht seine Zielbestimmung aus dem Auge.

Dies ist auch historisch zu erklären. Dem Datenschutzrecht lag vor dem Hintergrund der Entscheidung des Bundesverfassungsgerichts zur Volkszählung ursprünglich der Gedanke zugrunde, dass jede Verarbeitung personenbezogener Daten eine Gefährdung des Persönlichkeitsrechts mit sich bringt.[2] Zitat: „Kein Datum ist belanglos." Dieser Gedanke zielt darauf, sich stets rechtfertigen zu müssen, wenn man ein Datum verarbeitet. Eine allumfassende Rechtfertigung für sein Handeln verlangen wir zu Recht vom Staat.

2 BVerfGE 65, 1 ff. – Volkszählungsentscheidung.

Der Staat greift durch sein Handeln in Grundrechte ein und bedarf hierfür einer Rechtfertigung.

Ganz anders verhält es sich im privaten Bereich. Privatpersonen sind Grundrechtsträger. Aus ihrer Sicht bedeutet Datenverarbeitung die Ausübung einer grundrechtlich verbürgten Freiheit – zum Beispiel und mit Blick auf das Internet vor allem der Meinungsfreiheit –, die in den Grenzen der Grundrechte anderer zulässig sein muss. Es geht also um die Abwägung privater Rechte. Inhalt und Grenzen der Schutzpflicht des Staates sind auch rechtsdogmatisch von Ausgangspunkten her zu bestimmen, die sich von denen im Verhältnis Staat–Bürger deutlich unterscheiden. Die Debatte um die Drittwirkung von Grundrechten ist hier ein zentraler Aspekt.

Der herkömmliche Ansatz, das einzelne Datum zu schützen, ist somit im Privatbereich jedenfalls dann zunehmend problematisch, wenn der Schutzanspruch alle Lebensbereiche durchdringt und im schlimmsten Fall zur Bevormundung werden kann.

Bei der Frage nach der Zulässigkeit und Unzulässigkeit von Datenverarbeitungen rücken wir nach der Systematik des BDSG und des geltenden Europäischen Rechts auch im privaten Bereich das einzelne Datum in den Mittelpunkt und gehen davon aus, dass
- erstens kein Datum belanglos ist,
- zweitens möglichst wenig Daten verarbeitet werden sollen
- und man drittens Daten und ihre Verarbeitung jeweils getrennt in einzelnen Schritten bewerten und dabei Verantwortlichkeiten klar zuordnen kann.

Hier hat der Staat Schutzpflichten insbesondere in Bezug auf den einzelnen Internetnutzer, die zu definieren eine wichtige Aufgabe ist.

Diese Prämissen bedürfen im Informationszeitalter jedoch einer Überprüfung. Das rasante Wachstum des Internets läuft dem Grundsatz der Datenvermeidung und Datensparsamkeit ersichtlich zuwider. Niemand will dieses Wachstum ernsthaft aufhalten. Energieeinsparungen, Elektromobilität, digitale Partizipation, Meinungsäußerungen, Soziale Netzwerke und vieles mehr sind ohne die massenhafte Verarbeitung und Vernetzung von Daten nicht möglich. Durch den technischen Fortschritt werden die Daten insgesamt zunehmend personenbeziehbar. Hält man unter diesen Bedingungen jedes Datum für gleich wichtig und will jeden Schritt der Verarbeitung einzeln bewerten und regeln, stößt man spätestens bei der Rechtsumsetzung an Grenzen. Dies gilt erst recht im internationalen Kontext.

Die Rückbesinnung auf das Grundanliegen des Datenschutzrechts zeigt, dass es inhaltlich um ein „Privacy-Recht“ geht: Anstatt das einzelne Datum in den Mittelpunkt der Betrachtung zu rücken, sollte der Schutz der Privatsphäre unmittelbar im Zentrum der Regelungen stehen. Mit einem flexiblem Regelungsmodell könnte eine stärkere Konzentration auf die tatsächlichen Gefahren für die Privatsphäre der Betroffen möglich sein. Das Modell muss sich technischen Neuerungen schnell anpassen können. Bei Geschäftsmodellen oder Internetdiensten mit hohem Gefahrenpotenzial müssen schnell wirksame Schutzmechanismen greifen und strenge Regeln und Auflagen gelten. Hier hat der Staat Schutzpflichten insbesondere für den einzelnen Internetnutzer, die zu definieren eine wichtige Aufgabe ist. Weniger gefahrgeneigte Alltagsvorgänge sollten demgegenüber nicht unnötig einer „datenschutzrechtlichen Bürokratie“ unterworfen werden. Die automatisierte Buchhaltung eines kleinen Unternehmens zum Beispiel sollte nicht den gleichen Regelungen wie Facebook und Google unterliegen. Mit einer solch unterschiedslosen Herangehensweise wäre niemandem geholfen. Die gebotene Differenzierung aber ist unmöglich, wenn man auf das einzelne Datum abstellt. Das Anknüpfen an das einzelne Datum führt dazu, dass dem Betroffenen wahlweise zu viel Schutz aufgedrängt oder zu wenig Schutz geboten wird. Beides ist schlecht. Die Dosis macht das Gift. Dies gilt auch für die viel diskutierten Profilbildungen im Internet. Die Frage stellt sich, was zivilrechtlicher Regelung überlassen werden kann und was dem öffentlichrechtlichen Regime des Datenschutzes und seinen Eingriffs- und Überwachungsmechanismen unterstellt werden muss.

IV. Datenschutzrechtlicher und zivilrechtlicher Persönlichkeitsschutz

Nach dem Entwurf der EU-Kommission würden private Homepages, Blogs und Redebeiträge in Sozialen Netzwerken den gleichen Pflichten und Kontrollmechanismen unterstellt wie staatliche Behörden oder Großkonzerne. Hier ist – insbesondere mit Blick auf die Meinungs- und Pressefreiheit – aus meiner Sicht datenschutzrechtliche Zurückhaltung am Platz. Das gilt umso mehr, als es zum Schutz der Privatsphäre vor Verletzungen durch andere Privatpersonen bereits ein Instrumentarium gibt, das möglicherweise ausgebaut werden kann. Zu denken ist hier etwa an das Zivilrecht und bei Veröffentlichungen an das Äußerungs- und Presse- bzw. Medienrecht in seiner näheren Ausgestaltung und Konkretisierung durch die Rechtsprechung.

Wenn diese Instrumente konsequent zum Schutz der Privatsphäre eingesetzt und – soweit angesichts der Neuerungen des Informationszeitalters erforderlich – ergänzt werden, bedeutet dies keinen datenschutzrechtlichen Rückschritt. Es muss gemeinsam und europaweit gelingen, zu einem Datenschutz zu kommen, der einfach, verstehbar und anwendbar ist. Nicht die Ausrufung von Datenschutzskandalen im Internet nützt dem Bürger. Es sind verlässliche und praxisnahe Regeln, auf die er Anspruch hat und die der Staat entwickeln muss, wenn er seiner Verantwortung in der Informationsgesellschaft gerecht werden will.

Das EU-Datenschutzpaket: Keine Jahrhundertreform*

Dirk Heckmann

Inhaltsverzeichnis

I. Einleitung

1. Vorbemerkung: Das Projekt SCHUFALab@HPI

Wenn man wissen möchte, was die Menschen über aktuelle politische Themen denken, was ihre Interessen, Positionen, Erwartungen und Enttäuschungen sind, lohnt der Blick auf Twitter. Der längst auch dank Cross Media etablierte Kurznachrichten-Kanal ist so etwas wie ein Seismograf in der responsiven Demokratie,[1] sozusagen Noelle-Neumann 3.0.

Als ich in Vorbereitung dieses wissenschaftlichen Eröffnungsvortrags den Hashtag Datenschutz in Twitter eingab, galten die meisten deutschsprachigen Tweets dem geplanten und kurzfristig beendeten Forschungsprojekt

* Der Vortragsstil wurde beibehalten. Ich danke meinem Assistenten Axel Knabe für seine Mitarbeit.

1 Vgl. zu Fragen der responsiven Demokratie im Informationszeitalter *Heckmann*, Open Government – Retooling Democracy for the 21st Century, Proceedings of the 44th Hawaii International Conference on System Sciences, 2011; abrufbar unter http://ngis.computer.org/csdl/proceedings/hicss/2011/4282/00/04-05-05-abs.html.

SCHUFALab@HPI.[2] Die Spannbreite der Äußerungen reichte vom Vorwurf der Datenschutzwidrigkeit[3] über süffisante Verhaltenstipps zum Social Media Scoring bis hin zu blanker Beschimpfung der Schufa; das ganze garniert mit den üblichen Falschinformationen und Halbwahrheiten. Was den Forschungspartner, das HPI, betrifft, war man sich wiederum nicht sicher, ob man ihn schelten soll wegen der Projektidee oder loben wegen des Ausstiegs. Die Empörung im Netz war wohl auch deshalb so groß, weil es – neben der latenten Einschränkung freier Internetnutzung – wieder einmal um das Missverstehen von Internetanwendungen ging, aus dem dann sinnlose, unnötige oder unverhältnismäßige Eingriffe entstehen. Das war bei den leicht umgehbaren Netzsperren[4] so, und das zeigt sich auch bei dem Versuch, Erkenntnisse zur Kreditwürdigkeit ausgerechnet aus Informationen in den Sozialen Netzwerken zu ziehen. In der Tat liegt darin das stärkste Gegenargument gegen die Schufa-Idee. Zwar mag die Schufa auf den ersten Blick auf der Grundlage der §§ 28, 28b BDSG auf öffentliche Daten zugreifen dürfen. Jedoch müssten diese Daten (Pinnwandeinträge, Statusupdates, Fotos, Freundeslisten etc.) eine ausreichende Aussagekraft über die wirtschaftlichen Verhältnisse einzelner Personen haben. Das ist aber kaum der Fall. Zum einen sind die Nutzerkonten etwa auf Facebook vielfach nicht eindeutig zuordenbar, sie mögen in Einzelfällen sogar gefälscht sein. Zum anderen sind die genannten Informationen oft zweideutig, unscharf oder schlicht beliebig. Das Arbeitsgericht Dessau-Roßlau hat dies jüngst in einer Entscheidung zum Ausdruck gebracht, bei der es um die Kündigung eines Arbeitsverhältnisses ging, bei dem der Betroffene einen arbeitgeberkritischen Beitrag eines Dritten „geliked", also den „Gefällt-mir"-Button gedrückt hat. Ich zitiere: „Selbst wenn die Klägerin den fraglichen Button selber gedrückt hätte, wäre zu berücksichtigen, dass die Betätigung dieses Buttons bei Facebook-Nutzern in der Regel eine spontane Reaktion ohne nähere Überlegung darstellt und in ihrem Bedeutungsgehalt nicht zu hoch eingeschätzt werden sollte."[5] Ich möchte dies arbeits- und beweisrechtlich nicht näher erörtern. Dahingestellt sei auch, inwieweit hier das kolportierte Leitbild des dümmsten anzunehmenden Users zutreffend zugrunde gelegt wurde.[6] Wichtig ist

2 Vgl. zum Forschungsprojekt SCHUFALab@HPI: http://www.schufa.de/de/private/presse/aktuellepressemitteilungen/schufalab_hpi.jsp.

3 Kritisch zum Themenkreis Schufa und Datenschutz *Beckhusen*, BKR 2005, 335.

4 Vgl. zur Verfassungswidrigkeit des Zugangserschwerungsgesetzes *Heckmann/Heckmann*, jurisPK Internetrecht, 3. Aufl., 2011, Kap. 8, Rn. 56 ff.

5 ArbG Dessau-Roßlau, Urt. v. 21.3.2012 – 1 Ca 148/11.

6 Vgl. bezüglich der Nutzung Sozialer Netzwerke auch die Entscheidungen VG Ansbach, Beschl. v. 16.1.2012 – AN 14 K-11.02132 und ArbG Bochum, Urt. v. 29.3.2012 – 3 Ca 1283/11.