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.

die nun auch in der Judikatur angekommene Erkenntnis der fraglichen Validität von Informationen in den Sozialen Netzwerken. Deshalb vertrete ich auch die Auffassung, dass wegen des erheblichen Risikos einer Fehlinterpretation „das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt", § 28 Abs. 1 Nr. 3 BDSG, was das auf solche Daten gestützte Scoring nach § 28b Nr. 2 BDSG ausschließt.[7] Dies auch unter der Berücksichtigung der Tatsache, dass es sich bei den in Sozialen Netzwerken uneingeschränkt eingestellten Informationen um „öffentlich zugängliche" Daten im Sinne des Datenschutzrechts handelt. Diese sind nämlich mit der Veröffentlichung keineswegs zur allgemeinen Nutzung oder gar Ausbeutung freigegeben. Schon 1974 merkte *Walter Schmidt* zutreffend an, dass nicht nur die Vorenthaltung, sondern auch die Preisgabe personenbezogener Daten Grundrechtsausübung ist, die eine Sammlung und Speicherung solcher Informationen begrenzt.[8] Dies gilt fast 40 Jahre später erst recht im Zusammenhang mit Sozialen Netzwerken wie Facebook, bei denen der Kontext, in den Daten hineingestellt und weiter genutzt werden, diffus und das Geschäftsmodell intransparent ist.[9]

Dieser aktuelle Fall zeigt im Kleinen, welche Herausforderungen eine Datenschutzreform im Großen zu leisten hat.

2. Kurzüberblick zum EU-Datenschutzpaket

Am 25.01.2012 stellte die Europäische Kommission den Reformvorschlag für eine sogenannte Datenschutz-Grundverordnung vor,[10] der sich nun dem Gesetzgebungsverfahren stellen muss und die aus dem Jahre 1995 stammende Datenschutzrichtlinie 95/46/EG[11] ersetzen soll. Zugleich wurde auch ein Richtlinienentwurf zur Datenverarbeitung bei Polizei und Justiz[12] auf den Weg gebracht, auf den hier aber aus Zeitgründen nicht näher eingegangen werden kann.

---

7 Vgl. allgemein zu Fragen des Scorings *Wäßle/Heinemann,* CR 2010, 410.

8 *Schmidt*, JZ 1974, 241 (247).

9 Vgl. grundlegend zu diesen Fragen *Heckmann*, K & R 2010, 1.

10 Pressemitteilung EU-Kommission unter http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46 & format=HTML & aged=0 & language=DE.

11 Abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html.

12 Vgl. http://www.heise.de/newsticker/meldung/Reding-stellt-EU-Datenschutzreform-vor-1421418.html.

Der Entwurf zu einer Datenschutz-Grundverordnung – der zweifellos bisher umfassendste und in seinen Wirkungen weitreichendste europäische Reformansatz – setzt dabei in konsequenter Weise das mit dem Lissabon-Vertrag und der Grundrechtecharta der EU 2009 erteilte Mandat für eine umfassende Regelung des Datenschutzes auf allen Gebieten des EU-Rechts um.[13] Weitreichend ist der Entwurf der Grundverordnung dabei schon wegen seiner unmittelbaren Bindungswirkung, zunächst einmal abgesehen von den einzelnen materiellen Veränderungen, die mit ihm einhergehen könnten.

Denn im Gegensatz zur bisherigen Richtlinie bedarf die Verordnung keiner Umsetzung in das nationale Recht, sie gilt vielmehr in jedem europäischen Mitgliedsstaat unmittelbar. Den Mitgliedsstaaten würde es also grundsätzlich unmöglich werden, ihre datenschutzrechtlichen Regelungen im Geltungsbereich der Richtlinie in die eine oder andere Richtung auszudifferenzieren. Das bringt es zugleich mit sich, dass über entscheidende Auslegungsfragen letztlich der EuGH unter Berücksichtigung der EU-Grundrechtecharta entscheiden würde.[14] Dies wurde jüngst von Bundesverfassungsrichter Masing sehr kritisch kommentiert.[15] So ist unter anderem zu bedenken, dass es dem EuGH an einer beispielsweise dem deutschen Verfassungsrecht vergleichbaren, ausdifferenzierten Grundrechtsdogmatik bisher fehlt. Ebenso wie an einem der Verfassungsbeschwerde vergleichbaren Rechtsbehelf für den Einzelnen.

Natürlich gibt es auch zielführende Reformansätze. Um nur einige Punkte zu nennen, auf die ich nicht näher eingehen kann, die aber in Folgereferaten behandelt werden: Im materiellen Teil wird beispielsweise das Marktortprinzip statuiert (Art. 3 Abs. 2 DS-GVO-E), sodass die Regelungen der Verordnung auch für außereuropäische Datenverarbeiter gelten, soweit sie in der EU Waren oder Dienstleistungen anbieten. Weiterhin wird der Begriff der personenbezogenen Daten insofern ausgeweitet und festgelegt, als die Identifikation durch irgendeine – nicht zwangsläufig die verarbeitende Stelle – zur Qualifizierung als personenbezogenes Datum ausreicht (Art. 4 Abs. 1, 2 DS-GVO-E). Eine besonders „öffentlichkeitswirksame“ und vieldiskutierte Neuerung ist ohne Frage das Recht auf Vergessenwerden (Art. 17 DS-GVO-E),[16] auch wenn man hier durchaus den Vorwurf des Etikettenschwindels teilen kann: Es handelt sich weniger um ein praktisch umsetz-

13 Vgl. dazu *Reding*, ZD 2012, 195.
14 Vgl. *Hornung*, ZD 2012, 99 (100).
15 „Ein Abschied von den Grundrechten“, Süddeutsche Zeitung (SZ) v. 9.1.2012.
16 Vgl. dazu *Hornung*, ZD 2012, 99 (103).

bares Recht als vielmehr um eine bloße flankierende Informationspflicht.[17] Man kann ein Vergessen ebenso wenig gesetzlich anordnen wie man Erinnerungen im Gedächtnis erlebender Menschen löschen kann.[18]

Auch der Rechtsschutz bringt umfassende Regelungen bzw. Veränderungen mit sich, beginnend schon bei einer Meldepflicht gegenüber Aufsichtsbehörde und Betroffenem bei Datenschutzverletzungen (Art. 31, 32 DS-GVO-E). Zudem soll unter anderem ein Verbandsbeschwerde- und Klagerecht nach Art. 73 Abs. 2, Art. 76 Abs. 1 DS-GVO-E eingeführt werden. Sanktionen sollen sich auf bis zu eine Million Euro oder 2 % des weltweiten Jahresumsatzes erhöhen und nach derzeitiger Formulierung (Art. 79 DS-GVO-E) steht es zumeist nicht im Ermessen der Behörde, ob Bußgelder verhängt werden (die Höhe freilich schon).

Das EU-Datenschutzpaket ist keine Jahrhundertreform. In seiner jetzigen Fassung ist der Entwurf für eine EU-Datenschutzverordnung sicher ein Fortschritt in der Datenschutzdebatte, eine gewöhnliche Reform. Er würde aber keine Reform bewirken, die dieses Jahrhundert braucht. Das ist kein großer Wurf. Und dennoch ist er beachtlich. Im Prinzip wird ein umfassendes Datenschutzkonzept mit zahlreichen mehr oder weniger gelungenen Vorschriften als verbindliches Regelwerk aufgesetzt, das nationales Recht weitgehend verdrängt. Nachdem es künftig nur schwerfällig zu ändern sein wird, gilt es im Entstehungsprozess, die eigene Sicht der Dinge optimal einzubringen.[19] Mehr noch als in anderen politischen Themenfeldern sollte eine breite, konsensstiftende Diskussion mit allen Akteuren aus Politik, Wirtschaft, Gesellschaft und Wissenschaft geführt werden. Welche Punkte bei dieser Diskussion eine Rolle spielen sollten, möchte ich nun skizzieren.

17 So auch *Hornung*, ZD 2012, 99 (103).

18 Vgl. schon zur Diskussion um den sog. „digitalen Radiergummi", *Simitis/Dix*, BDSG, 7. Aufl., 2011, § 35 BDSG, Rn. 8; *Nolte,* ZRP 2011, 236; *Hoeren,* ZRP 2010, 251; *Härting/Schneider,* ZRP 2011; *Bull,* NVwZ 2011, 257.

19 Zu Fragen der Transparenz und Mitwirkung in multinationalen Abstimmungs- und Entscheidungsprozessen am Beispiel ACTA vgl. „Aufstand der Unverstandenen", Legal Tribune Online (LTO) v. 10.2.2012. http://www.lto.de/recht/hintergruende/h/stopp-acta-aktionstag-aufstand-der-unverstandenen/.

II. Eckpunkte für ein zeitgemäßes Datenschutzrecht

Was sind die Eckpunkte, mit denen sich die Reformdiskussion auseinandersetzen sollte? Ich möchte vier Punkte hervorheben, ohne deren Klärung kein wirklicher Fortschritt erzielt werden kann. Es geht um

- das Verbotsprinzip vor dem Hintergrund rechtsstaatlicher Fürsorge,
- das Einwilligungsmanagement vor dem Hintergrund informationeller Selbstbestimmung,
- Privacy by Design vor dem Hintergrund des Verlusts rechtlicher Steuerungskraft und
- Strategien zur Missbrauchserkennung und Missbrauchsabwehr vor dem Hintergrund des verfassungsstaatlichen Rationalitätspostulats.

1. Was soll eigentlich geschützt werden? Und warum?

Zunächst stellt sich die Frage, was in einem zeitgemäßen Datenschutzrecht überhaupt geschützt werden soll und warum dies geschieht. Die Antwort lieferte im überkommenen nationalen und supranationalen Recht das sog. Verbotsprinzip. Danach dürfen personenbezogene Daten nur dann erhoben, verarbeitet und genutzt werden, wenn dies gesetzlich oder durch explizite Einwilligung erlaubt ist, so etwa § 4 Abs. 1 BDSG.[20] Kurz: Im Datenschutzrecht ist alles verboten, was nicht ausdrücklich erlaubt ist. Daran soll nach dem Entwurf zur Datenschutzverordnung nichts geändert werden, wie Art. 6 Abs. 1 deutlich macht. Damit ignoriert der Reformgesetzgeber eine seit geraumer Zeit auch in juristischen Fachkreisen geführte Diskussion, die viele Namen, aber im Wesentlichen zwei Gesichter hat.

Niko Härting und *Jochen Schneider* setzen sich seit Jahren für eine Modernisierung des Datenschutzes ein und setzen dabei sozusagen „ganz vorne" an, nämlich bei der Frage, was in Bezug auf die Datenverarbeitung im Internetzeitalter grundsätzlich erlaubt und was eher verboten sein soll. Sie sehen Vorteile in einer zumindest teilweisen Aufhebung des Verbotsprinzips. Dieses sei nicht „internettauglich" und behindere die freie Kommunikation und unternehmerische Betätigung übermäßig.[21] Zwar sei die Vorstellung, jede Art der „datengestützten Kommunikation" brauche eine gesonderte Rechtfertigung, seit dem Volkszählungsurteil so stark verfestigt, dass man sie nur

20 Vgl. allgemein zum Verbotsprinzip *Redeker,* in: Redeker (Hrsg.), IT-Recht, 2012, S. 309.

21 Vgl. dazu die Ausführungen von *Schneider/Härting* auf http://www.schneider-haerting.de/2011/09/leitlinien-des-datenschutzes/.

schwer infrage stellen könne. Keineswegs liefere aber nur ein auf das Verbot mit Erlaubnisvorbehalt gestütztes Datenschutzrecht gute und zukunftstaugliche Ergebnisse. Im Gegenteil: Es ignoriert ihrer Ansicht nach die unterschiedliche Bedeutung und Arten von Daten sowie ihren oftmals kommunikations- und damit grundrechtsausübungsbezogenen Charakter.[22] Das Medienprivileg – ob in der Verordnung (Art. 80 DS-GVO-E) oder im nationalen Datenschutz – sei ein Instrumentarium aus Zeiten vor dem Social Web und in seinen Details zu streitig, als dass es das Verbotsprinzip in grundrechtskonformer Weise auflockern könne.[23] Mehr möchte ich an dieser Stelle nicht sagen, zumal Herr Kollege *Härting* ja später selbst referieren wird.

An die von *Härting* und *Schneider* vorgebrachte Skepsis anknüpfend möchte ich aber meine erste These formulieren:

These 1: Das Verbotsprinzip kollidiert im privaten Sektor mit den Anforderungen an ein zeitgemäßes, wirksames und interessengerechtes Informationsmanagement. Die notwendige neue Weichenstellung erlaubter und verbotener Formen der Datenverarbeitung und des Informationszugriffs ist nach einer breiten gesellschaftlichen Debatte über das Leitbild der Informationsgesellschaft und die Grenzen des digitalen Wachstums vorzunehmen.

Die Einschränkung auf Datenverarbeitung im privaten Sektor versteht sich von selbst. Der Daten verarbeitende und die Datenpreisgabe vor allem erzwingende Staat ist schon wegen der Grundrechtsbindung daran gehindert, ohne gesetzliche oder individuelle Erlaubnis auf Daten seiner Bürger zuzugreifen.[24] Deshalb beschränke ich mich in meinen Ausführungen auf den ohnehin viel spannenderen, dynamischen privaten Sektor, vor allem auf die Datenverarbeitung und Datennutzung im Internet.

Insoweit bin ich mir nicht sicher, ob wir das Verbotsprinzip wirklich problemlos umkehren können, nach dem Motto: Jegliche Datenverarbeitung ist erlaubt, soweit sie nicht explizit durch Gesetz oder den Betroffenen verboten ist. Dies setzt idealtypisch einen rationalen Umgang des Gesetzgebers mit neuen Gefährdungslagen, innovativen Nutzungsformen und politischen Leitideen voraus. Wenn er nicht oder falsch reagiert, riskiert er die Verletzung staatlicher Schutzpflichten.[25] Um also die grundrechtlich garantierte

22 Hierzu auch *Härting*, K & R 2012, 264 (266 ff.).

23 Ebd.

24 Vgl. *Gurlit*, NJW 2010, 1035 (1040).

25 Zu Schutzpflichten allgemein *Stern*, DÖV 2010, 241. In Bezug auf das Grundrecht auf informationelle Selbstbestimmung und zum IT-Grundrecht *Heckmann*, in: FS f. Käfer, 2009, S. 129.

Privatsphäre[26] und den Persönlichkeitsschutz[27] zu gewährleisten, bedarf es einer durchaus begrenzten Regulierung des Datenverkehrs: So wenig wie möglich, aber so viel wie nötig. Die Wahrheit liegt also irgendwo zwischen dem Übermaßverbot und dem Untermaßverbot. So etwas wie webbasiertes Scoring zum Beispiel kann sicher nicht der normativen Kraft des Faktischen überlassen werden. Auch sonst ist die Erhebung und Nutzung spezifischer Nutzerprofile, zum Beispiel als Bewegungs- oder Konsumprofile,[28] ein heikles Thema. Und so gibt es viele Spannungsfelder, die bei Abschaffung des Verbotsprinzips einer demokratischen Auflösung harren.

Es gibt aber noch ein weiteres Argument, weshalb es einer gesellschaftlichen Debatte und nachfolgender gesetzlicher Weichenstellung bedarf: Das digitale Wachstum darf nicht grenzenlos sein, genauso wenig wie die damit verbundene Datenverarbeitung und Datennutzung. Mit dieser Begrifflichkeit möchte ich an die berühmte Studie zur Zukunft der Weltwirtschaft[29] erinnern, die 1974 im Auftrag des Club of Rome erstellt wurde[30] und mittlerweile zwei Updates erhalten hat.[31] Natürlich lassen sich die Situationen nicht ganz vergleichen (hier etwa die zunehmende Digitalisierung, Automatisierung, Zentralisierung und Vernetzung, einhergehend mit einem Verlust an persönlicher Autonomie und Privatheit, dort das Bevölkerungswachstum, Ausbeutung natürlicher Ressourcen etc.). Mir geht es auch nicht um einen durchaus hinkenden Vergleich der *Ausgangslagen*, sondern um den vergleichbaren *Appell*, auch über die Spätfolgen der Prozesse nachzudenken, die derzeit mit rasanter Geschwindigkeit ablaufen und die aufgrund ihrer volkswirtschaftlichen Bedeutung, hohen und sofortigen Nützlichkeit und zahlreichen Verführungskomponenten wenig reflektiert werden.

Dem „heilsbringenden" Charakter ständiger digitaler Expansion sollten wir nicht blind vertrauen, die Wachstumsgrenzen gerade auch mit Blick auf die Abschätzung von Spätfolgen jedenfalls entsprechend berücksichtigen.

---

26 Zum grundrechtlichen Privatsphärenschutz vgl. *Maunz/Dürig/Di Fabio*, GG, 64. Ergänzungslieferung 2012, Rn. 149 ff.

27 Zum grundrechtlichen Persönlichkeitsschutz vgl. *Maunz/Dürig/Di Fabio*, GG, 64. Ergänzungslieferung 2012, Rn. 127 ff.

28 Zu Fragen der Nutzerprofile vgl. *Rasmussen,* CR 2002, 36.

29 Siehe zu der Studie die „Grenzen des Wachstums" http://www.nachhaltigkeit.info/artikel/meadows_u_a_die_grenzen_des_wachstums_1972_1373.htm.

30 Zur ursprünglichen Studie siehe *Hahn,* Von Unsinn bis Untergang: Rezeption des Club of Rome und der Grenzen des Wachstums in der Bundesrepublik der frühen 1970er Jahre, 2006.

31 Zu den Updates siehe *Seiler,* Von den Grenzen des Wachstums zur Überforderung der ökologischen Tragfähigkeit, Natur und Kultur, 3 ff.; abrufbar unter http://www.umweltethik.at/download.php?id=326.

Zugleich aber darf der Gesetzgeber das Wachstum des digitalen Raumes auch nicht übermäßig verkürzen. Interessengerechte Einwilligungslösungen bei Datenverarbeitungen müssen durch eine zukunftsweisende Neujustierung erlaubnistatbestandlicher Fragen flankiert werden.

Ob das dann über die Abschaffung, Umkehrung bzw. Relativierung des Verbotsprinzips oder eine Erweiterung der geregelten Erlaubnistatbestände erreicht werden soll, kann erst nach einem breit angelegten gesellschaftlichen Dialog über diese Fragen entschieden werden. Die Kunst besteht darin, komplexe juristische Strukturen in ent- bzw. unterscheidbare politische Konzepte zu übersetzen.

2. Wie kann man den Einzelnen wirksam schützen?

Dies führt mich zum zweiten Eckpunkt eines zeitgemäßen Datenschutzrechts, dem Einwilligungsmanagement. Es ist ein eherner Grundsatz des Datenschutzrechts, dass personenbezogene Daten außerhalb gesetzlicher Festlegungen nur dann verarbeitet werden dürfen, wenn der Betroffene eingewilligt hat.[32] So in § 4 BDSG, § 12 TMG und nun auch in Art. 6 Nr. 1 a, Art. 7 des Entwurfs zur Datenschutz-GVO. Das klingt in der Theorie sehr plausibel, setzt es auf den ersten Blick doch das Grundrecht auf informationelle Selbstbestimmung[33] um. Schließlich soll, wie schon das Volkszählungsurteil[34] formulierte, jeder selbst entscheiden, wer wann was über ihn weiß. Nur sieht das in der Praxis anders aus. Die Einwilligung zu möglicherweise erheblicher Datenverarbeitung wird in der Regel mit einem Klick buchstäblich abgehakt. Nachdem man bestenfalls mehrere Bildschirmseiten Datenschutzbestimmungen heruntergescrollt hat.[35]

Nun könnte man meinen, dies sei doch nichts anderes als informationelle Selbstbestimmung. Niemand sei gezwungen, lange und wenig verständliche juristische Texte zu lesen. Umgekehrt könne auf diese Texte nicht verzichtet werden, da in ihnen insbesondere die für die Zweckbestimmung und Zweckbindung notwendigen Angaben enthalten seien. Diese Argumentation erscheint mir allerdings etwas zynisch. Wenn man den Grundrechtsschutz, der gerade in unserem Kontext auch Grundrechtsschutz durch Ver-

32 *Taeger/Gabel/Taeger,* BDSG, 2010, § 4 BDSG, Rn. 43; *Menzel,* DuD 2008, 400 (401).

33 Zum informationellen Selbstbestimmungsrecht vgl. *Gola/Schomerus,* BDSG, 10. Aufl., 2010, § 1 BDSG, Rn. 9 ff.

34 BVerfG, NJW 1984, 422.

35 Zur Kritik an unübersichtlichen Datenschutzbestimmungen vgl. *Meyer*, K & R 2012, 309 (310).

fahren[36] bedeutet, ernst nimmt, darf man die Einwilligung nicht auf eine Formalie reduzieren, hinter der keine wirklich fundierte Entscheidung steht. Der in der informationellen Selbstbestimmung liegende Gedanke autonomer Lebensgestaltung[37] setzt eine Auswahlsituation voraus, in der eine bewusste Disposition getroffen wird und überhaupt getroffen werden kann: sei es zugunsten oder zuungunsten der intendierten Datenverarbeitung. Und genau hier liegt das Dilemma, das ich die Plug-and-Play-Falle[38] nenne:

Datenintensive IT-, insbesondere Internetapplikationen werden immer beliebter, weil
- sie sehr nützlich sind oder zumindest so erscheinen,
- vielfach unterhaltsam sind, auf jeden Fall leicht zu bedienen und
- vielfach unentgeltlich sind.

Darauf aufbauend werden permanent neue Applikationen geschaffen und vielfach miteinander verknüpft, was wiederum neuen Nutzen und Spaß schaffen kann. Entsprechende Geschäftsmodelle versprechen hohe Rendite, was sich ja nicht gleich in überzeichneten Aktien äußern muss.

Diese Entwicklung wird durch passende Hardware unterstützt, die wie etwa das iPhone, das iPad oder auch Nobelgeräte auf Windows- oder Android-Basis Kultcharakter bekommen. Dieses Must-have beflügelt die Hersteller und Entwickler und weckt wiederum die Erwartungshaltung beim eher unkritischen Publikum. Der Vertrieb wird ebenfalls erleichtert, versprechen Jubelbeiträge in Print- und Online-Medien sowie Funk und Fernsehen inzwischen auch höhere Auflagen, Einschaltquoten und Klickraten. Dem kann sich die Politik kaum entziehen, will man mit kritischen Tönen zu Facebook, Google & Co. doch keinen Shitstorm[39] riskieren, der die Wiederwahlchancen reduziert.

Wenn aber die Wirtschaft, die Nutzer, die Medien und die Politik gleichermaßen an einem Strang ziehen, finden Datenschutzbedenken kaum Gehör. Business as usual! Durch die Plug-and-Play-Falle ist der unreflektierte, uninformierte Klick auf die Einwilligung vorprogrammiert. Die IT-Gesell-

---

36 Vgl. dazu allgemein *Gurlit*, NJW 2010, 1035 (1039); *Polenz,* in: Kilian/Heussen (Hrsg.), Computerrecht, 2011, Rn. 1 ff.; Kahl, VerwArch 2004, 1 ff.

37 Vgl. BVerfG, NJW 1984, 422.

38 Vgl. dazu schon *Heckmann*, K & R 2010, 1.

39 Vgl. weiterführend zum Phänomen des „Shitstorms" und möglichen juristischen Folgefragen Schwenke, K & R 2012, 305; „Hass-Tweets vom Stammtisch", The European v. 22.5.2012. Abrufbar unter http://www.theeuropean.de/dirk-heckmann/11145-juristische-betrachtung-des-shitstorms.