Meike Kamp, Martin Rost

Kritik an der Einwilligung

Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen.

1 Einleitung

Einer Manipulierbarkeit durch die Verarbeitung personenbezogener Daten sollen die Betroffenen ihr Recht entgegensetzen können, selbst über die Zulässigkeit und die Modalitäten des Zugriffs auf ihre Daten zu befinden.[1] Das Recht auf informationelle Selbstbestimmung eröffnet für den Einzelnen nicht nur die Möglichkeit zwischen Zustimmung und Ablehnung zu wählen, sondern stellt nach Funktion und Bedeutung ein Gestaltungs- bzw. Mitwirkungsrecht dar. Einfachgesetzlich soll die datenschutzrechtliche Einwilligung „genuiner Ausdruck"[2] des verfassungsrechtlich garantierten Rechts auf informationelle Selbstbestimmung des Betroffenen sein.

In der Praxis ist die Einwilligung weit davon entfernt, diesen Erwartungen gerecht zu werden. Zumindest in Beziehungen zwischen Organisationen und Betroffenen mit asymmetrischen Machtverhältnissen erschöpfen sich die Bestimmungsmöglichkeiten der Betroffenen darin, zu einem vom Datenverarbeiter diktierten Sachverhalt entweder „Ja" oder „Nein" zu sagen. Ein informationeller Selbstschutz durch die Einwilligung versagt gänzlich, wo die Verweigerung der Einwilligung zur Ablehnung des Vertragsschlusses führt, auf den es den Betroffenen in der Regel ankommt.

1 Simitis in: Simitis (Hrsg.), BDSG, § 1 Rn. 26.
2 Roßnagel/Pfitzmann/Garstka, Modernisierungsgutachten, 2001, S. 72.

Meike Kamp, LL.M.

Referentin beim Berliner Beauftragten für Datenschutz und Informationsfreiheit

E-Mail: kamp@datenschutz-berlin.de

Martin Rost

Mitarbeiter im Referat „Systemdatenschutz" beim Unabhängigen Landeszentrum für Datenschutz (ULD) in Kiel.

E-Mail: martin.rost@datenschutzzentrum.de

Die Kritik an der Schutzwirkung der Einwilligung ist ebenso alt[3] wie aktuell. Zum Teil wird die Einwilligung als „Fiktion" bezeichnet.[4] Derzeit wird das Thema im Zusammenhang mit der Datenschutz-Grundverordnung[5] intensiv diskutiert. Der Verordnungsentwurf versucht das Problem in Art. 7 Abs. 4 einzukreisen. Dort heißt es, dass die Einwilligung keine Rechtsgrundlage für die Verarbeitung bietet, wenn zwischen der Position des Betroffenen und des für die Verarbeitung Verantwortlichen ein *erhebliches Ungleichgewicht* besteht. Wir möchten diesem aus unserer Sicht konzeptionell mutigen Schritt in die richtige Richtung ein paar Überlegungen mitgeben und insbesondere aufzeigen, dass durch den Einsatz von Einwilligungen in asymmetrischen Verhältnissen eine weitere Gefahr entsteht: Einwilligungen, die für die Betroffenen keine Schutzwirkung entfalten und eine belastbare Rechtsgrundlage nur simulieren, schädigen die Allgemeinheit, indem sie die gesellschaftlichen Quellen der informationellen Selbstbestimmung, nämlich Markt, Gewaltenteilung und Demokratie sowie freie Diskurse unterlaufen.

2 Erhebliches Ungleichgewicht

Im öffentlichen Bereich besteht ein Ungleichgewicht zwischen der Position des Betroffenen und der verantwortlichen Stelle immer dann, wenn Bürger und Staat im Subordinationsverhältnis zueinander stehen. Dieses Verhältnis ist gesetzlich geregelt. Anders liegt der Fall, wenn Bürger und Staat sich als gleichberechtigte Partner begegnen, etwa bei öffentlich-rechtlichen Verträgen.

Im nicht-öffentlichen Bereich besteht dann ein erhebliches Ungleichgewicht, wenn die verantwortliche Stelle eine *Monopolstellung* innehat, der Betroffene von der Organisation *abhängig* ist oder ein *informationelles Ungleichgewicht* existiert und die Einwilligung jeweils an den Abschluss des Vertrags gekoppelt ist.

Im Fall einer Beziehung zu einem Monopolisten bedeutet die Verweigerung der Einwilligung durch den Betroffenen schlicht, dass er die begehrte Leistung nirgendwo anders bekommt.

Abhängigkeitsverhältnisse sind dadurch gekennzeichnet, dass es für den Betroffenen zur Sicherung seiner persönlichen Lebensverhältnisse[6] unzumutbar ist, auf die Leistung zu verzichten. Roßnagel, Pfitzmann und Garstka sprechen im Modernisierungsgutachten von 2001 von „(Infrastruktur-) Leistungen der zivilisatorischen Grundversorgung", bei denen zu vermuten sei, dass die Einwilligung nicht freiwillig erfolgt, wenn sie an das Vertragsver-

3 Roßnagel/Pfitzmann/Garstka, Modernisierungsgutachten, 2001, S. 91; Sokol in: Simitis (Hrsg.), BDSG, § 4a Rn. 3.
4 Sokol in: Simitis (Hrsg.), BDSG, § 4a Rn. 3.
5 KOM/2012/011 endgültig.
6 Vgl. BVerfG 1 BvR 2027/02 vom 23.10. 2006, Absatz –Nr. 36.

hältnis gekoppelt ist.[7] Als Beispiele für solche Leistungen dienten Telekommunikation, Internetzugang, Kranken- und Rentenversicherung, Girokonto, Kredikarte und medizinische Versorgung.[8] Hierzu können auch andere Versicherungen[9] oder z. B. Energieversorgungsleistungen zählen. Darüber hinaus sind existentielle Abhängigkeiten auch im Arbeitsverhältnis und ggf. in Mietverhältnissen gegeben. Zudem können zukünftig Leistungen, die andere Aspekte der Lebensgestaltung betreffen, zur Grundversorgung zählen.[10] So ist vorstellbar, dass die Teilnahme am Social-Web für die „soziale Grundversorgung" unentbehrlich wird, weil ansonsten kommunikative Ausgrenzung droht.

Ein „informationelles Ungleichgewicht" stellt sich ein, wenn Organisationen Verkettungsmacht oder Deutungshoheit besitzen oder die operativen Regeln im Hard- und Softwarebereich bestimmen. Verkettungsmacht ist dann zu vermuten, wenn die Organisation sich mit einer Vielzahl von Dienstleistungen und Produkten an die Betroffenen wendet und in der Lage ist, z. B. über das Modell des „unique users"[11] oder über „social plugins" Betroffene auch ohne Klarnamen produkt- oder dienstleistungsübergreifend zu identifizieren[12] und die digitalen Aktivitäten des Betroffenen oder seine Beziehungsgeflechte („social graph") zu dokumentieren. Deutungshoheit hat, wer bestimmt, was im Netz gesucht werden kann (z. B. durch einen Begriffvorschlag bei der Eingabe in die Suchmaschine) und was wie als Treffer an welcher Position angezeigt wird. Dies entscheidet darüber, welche Unternehmen im Internet auf dem Markt adressabel sind. Die operativen Regeln werden durch die Hersteller von Hard- und Software bestimmt, an deren Produkten der Betroffene für seine digitalen Aktivitäten weder im Privat- noch im Arbeitsleben vorbeikommt. Das bedeutet z. B., dass die Nutzung von etwas zur „geübten Alltagspraxis" wird (bestimmte Betriebssysteme, Social-Web, ggf. Smartphones und Apps). Wer davon keinen Gebrauch macht, droht sich durch technische Inkompatibilität bzw. faktische Vernetzungs- und Verbindungsunfähigkeit gesellschaftlich ins Abseits zu stellen.

3 Fiktionen bei der Einwilligung

Mit den Kriterien der Freiwilligkeit, der Bestimmtheit und Informiertheit (§ 4a BDSG) sind Anforderungen an eine Einwilligung gestellt mit dem Zweck, dass von diesen für den Betroffenen eine kalkulierbare Schutzwirkung ausgeht. In asymmetrischen Machtverhältnissen entpuppen sich diese Wirksamkeitsanforderungen jedoch durchweg als Fiktionen.

3.1 Freiwilligkeitsfiktion

Roßnagel, Pfitzmann und Garstka schlugen vor, dass eine Vermutung dafür spricht, dass es an der Wirksamkeitsanforderung der „Freiwilligkeit" der Einwilligung mangelt, wenn eine Leistung der zivilisatorischen Grundversorgung von der Einwilligung der betroffenen Person in die Verarbeitung ihrer Daten abhängig gemacht wird.[13] Gleiches sollte gelten, wenn die Einwilligung in dauerhaften Abhängigkeitsverhältnissen eingesetzt werden soll. Das BVerfG sieht ebenfalls Handlungsbedarf, wenn es für den Betroffenen unzumutbar ist, zur Vermeidung der zu weitgehenden Preisgabe persönlicher Informationen, die angebotene Leistung, die für die Sicherung seiner persönlichen Lebensverhältnisse von erheblicher Bedeutung ist, auszuschlagen.[14] In solchen Abhängigkeitsverhältnissen fehlt es folglich an der Freiwilligkeit der Einwilligung.

Letztlich gerät die Freiwilligkeit bereits dann ins Wanken, wenn nicht gewährleistet ist, dass sich der Betroffene gegen die Einwilligung aussprechen kann und trotzdem ein Handel mit dem Unternehmen zustande kommt (*Wahlfreiheitsfiktion*). Die Zwangslage besteht dann (bestenfalls) darin, dass der Betroffene Nachteile eines unnützen Aufwandes oder Zeit- und Geldverlusts vermeiden möchte, und die Preisgabe seiner Daten daher in Kauf nimmt.[15]

Die Wahlfreiheit ist insbesondere dort nicht gegeben, wo der Handel aus Sicht der Organisation gerade darin besteht, dass die Leistung im Gegenzug für die Preisgabe der personenbezogenen Daten erfolgt, obwohl diese Sichtweise, auch unter dem Gesichtspunkt der Privatautonomie, nicht tragfähig ist. Die Privatautonomie hat ihre Grenzen dort, wo das Individuum schutzbedürftig ist,[16] d. h. sich die Ausstrahlungswirkung der Grundrechte im Zuge der mittelbaren Drittwirkung erhöht.[17] Dies soll dann der Fall sein, wenn es um den „Schutz personaler Freiheit gegenüber wirtschaftlicher und sozialer Macht" geht bzw. sobald „sehr ungleiche Verhandlungsstärken zum Tragen kommen", also immer dann, wenn das „der Privatrechtsordnung immanente Prinzip des Machtgleichgewichts verschiedener Privatrechtssubjekte gestört ist oder keine Möglichkeiten zum Selbstdatenschutz" bestehen.[18] Dies ist typischerweise in den Fällen des informationellen Ungleichgewichts gegeben, insbesondere sind Medien- und Technologieunternehmen als „Träger sozialer Macht" zu identifizieren.[19]

Zu einer anderen Einschätzung im Hinblick auf die Wahlfreiheit könnte man nur dann gelangen, wenn ein Markt bestünde, auf dem andere Unternehmen „echte" Alternativen anbieten, d. h. wenn Wettbewerb über datenschutzrechtliche Konditionen herrscht.[20] Aber auch dies ist eine Fiktion (*Marktfiktion*): Der Markt müsste dabei in dem Sinne perfekt sein, dass Transparenz bzgl. der Compliance mit Datenschutzrecht und zumindest ein tatsächlich überprüfbar datenschutzgerechtes Ange-

7 Roßnagel/Pfitzmann/Garstka, Modernisierungsgutachten, 2001, S. 95.

8 Roßnagel/Pfitzmann/Garstka, Modernisierungsgutachten, 2001, S. 95.

9 In dem Beschluss des BVerfG 1 BvR 2027/02 vom 23.10.2006 ging es um eine Berufsunfähigkeitsversicherung.

10 Zur Wandlung des Begrifs „Daseinsvorsorge" siehe Luch/Schulz, „eDaseinsvorsorge – Neuorientierung des überkommenen (Rechts-)Begriffs „Daseinsvorsorge" im Zuge technischer Entwicklungen", MMR 2009, 19.

11 Rost, „Gegen große Feuer helfen große Gegenfeuer", Vorgänge, Heft 4/2008, Nr. 184, 15-25.

12 Karg/Thomsen,„Tracking und Analyse durch Facebook", DuD, Heft 10, 729-736.

13 Roßnagel/Pfitzmann/Garstka, Modernisierungsgutachten, 2001, S. 91.

14 So das BVerfG in 1 BvR 2027/02 vom 23.10.2006, Absatz-Nr. 36, zu den Ursachsen „einseitiger Bestimmungsmacht" eines Vertragsteils.

15 Siehe Erwägungsgrund 33 des Entwurfs der Datenschutz-Grundverordnung: Echte Wahlfreiheit soll nur dann bestehen, wenn der Betroffene in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch *Nachteile* zu erleiden.

16 Dix in : Simitis (Hrsg.), BDSG, § 6 Rn. 14.

17 Luch, „Das neue „IT-Grundrecht" Grundbedingung einer „Online-Handlungsfreiheit", MMR 2011, 75 (78).

18 Luch, „Das neue „IT-Grundrecht" Grundbedingung einer „Online-Handlungsfreiheit", MMR 2011, 75 (78) mit weiteren Nachweisen.

19 Da deren Möglichkeiten der politischen, gesellschaftlichen und geistigen Einflussnahme unbestreitbar seien, so Luch, „Das neue „IT-Grundrecht" Grundbedingung einer „Online-Handlungsfreiheit", MMR 2011, 75 (78) mit weiteren Nachweisen; vgl. auch Ausführungen zur Deutungshoheit unter Punkt 2.

20 Für den Versicherungsfall schließt das BVerfG dies in 1 BvR 2027/02 vom 23.10.2006, Absatz-Nr. 40 aus.

bot besteht. Allerdings ist dann damit zu rechnen, dass ein ggf. aufwändigeres, datenschutzgerechtes Verfahren eines anderen Unternehmens möglicherweise nur zu einem höheren Preis angeboten wird, und damit unattraktiver ist. Gesetzeskonformität wird so zum Nachteil für Unternehmen.

3.2 Bestimmtheits- und Transparenzfiktion

Angenommen, die Einwilligung wäre freiwillig zustande gekommen, dann könnte sich eine direkte Schutzwirkung einstellen, wenn aufgrund der Transparenzpflichten ein Druck auf die Organisation wirkt, eine enge Zwecksetzung vorzunehmen und bspw. sämtliche Empfänger von Daten anzugeben sowie die Risiken der Datenverarbeitung anhand etwa des Standard-Datenschutzmodells mit den Schutzzielen des Datenschutzes und der Datensicherheit mit den entsprechenden Schutzmaßnahmen auszuweisen.[21] Eine tatsächliche Transparenz in all die beteiligten Datenbestände und Schnittstellen, IT-Systeme und Software, Prozesse und Organisationsstrukturen, Vertrags-, Verantwortungs- und Vertrauensverhältnisse zu bekommen, überfordert dabei allerdings nicht nur Laien. Bereits auf einem einzelnen PC können Zusammenhänge, die sich allein auf die Datenflüsse beziehen, komplex sein.

Hiergegen könnte argumentiert werden, dass es den Organisationen möglich wäre – wenn sie nur wollten – konkret darzulegen und dies den Betroffenen in angemessener Weise verständlich zu machen (z.B. durch nach Umfang und Detaillierungsgrad gestaffelte Informationen), und z. B. durch die Verteilung auf verschiedene Informationsstufen (bzw. Informationslevel „Einstieg" bis „erweitert") die Verständlichkeit und Transparenz der Informationen erreicht werden könnte. Dieser Einwand vermag allerdings nicht zu überzeugen, angesichts von Geschäftsmodellen, die darauf angelegt sind, personenbezogene Daten ohne Zweckbindung, ohne Beschränkung des Umfanges und ohne Erforderlichkeit auf Vorrat zu sammeln. Diese Fälle vertragen sich nicht mit der einen konkreten Zweck voraussetzenden, bestimmten und transparenten Einwilligung.

Die Aufsichtsbehörden haben die Aufgabe, als Stellvertreter für die Betroffen sachkundige Prüfungen durchzuführen und ihre Ergebnisse dann zu veröffentlichen. Insofern muss der Betroffene sowohl in eine Organisation als auch in die Kompetenz, Transparenz und Integrität der Aufsichtsbehörden vertrauen. Deshalb ist es hier angemessen, insgesamt von einer *Transparenz- bzw. Bestimmtheitsfiktion* zu sprechen.

3.3 Aufsichtsfiktion

Die *Aufsichtsfiktion* kann Mehreres bezeichnen, unter anderem, dass Betroffene darauf vertrauen, dass gerade große Organisationen es sich nicht leisten können, gegen geltendes Recht zu verstoßen, ohne dass Aufsichtsbehörden davon Kenntnis erlangen. Ein Betroffener geht das für ihn vielleicht durchaus ersichtliche Risiko einer Einwilligung in dem Glauben ein, dass er in einem Schadensfall zu seinem Recht kommen wird. Genau das kann in der aktuellen Situation klar infrage gestellt werden, wenn man sich allein die Zuständigkeitsproblematiken von Aufsichtsbehörden bei außereuropäischen Unternehmen vergegenwärtigt oder z. B. an die Schwierigkeiten im Falle von facebook denkt, eine gerichtliche Klärung herbei zu führen. Darüber hinaus können die Aufsichtsbehörden aufgrund ihrer geringen personellen und sachlichen Mittel die in sie gesetzten Erwartungen häufig nicht erfüllen.

4 Zwischenfazit

Man kann festhalten, dass die normativen Anforderungen an die Einwilligung bei asymmetrischen Machtverhältnissen nicht nur nicht erfüllt werden, sondern mehr noch, gar nicht erfüllbar sind. Einwilligungen basieren dann durchweg auf reinen Fiktionen, die keine kalkulierbaren oder kontrollierbaren Schutzwirkungen aufweisen. Fiktionen sind nicht prüfbar. Sie verhelfen nicht dazu, dass die Aktivitäten von Organisationen unter Bedingungen gestellt, d. h. beherrschbar und vertrauenswürdig werden. Im Gegenteil: Die Fiktionen der Einwilligung führen dazu, dass die konkrete, tatsächliche Ausgestaltungsmacht der personenbezogenen Verfahren vollständig und ungebrochen bei den Organisationen liegt. Die Einwilligung stellt damit ein Datenschutzrisiko für den Betroffenen und die Allgemeinheit dar. Die mit Abstand klarste und wirkungsvollste Regelung des Datenschutzrechts, das Verbot mit Erlaubnisvorbehalt, wird von der Einwilligung unterlaufen. Die Organisationen lassen sich aufgrund ihrer Macht im Einzelverhältnis die auf Fremdbestimmung ausgelegten Datenverarbeitungen durch die einzelnen Kunden jeweils genehmigen und entziehen sich damit einer systematischen Gesamtüberprüfung nach gesetzlichen Vorgaben.

Die Aktivitäten des Datenschutzes zielen nicht ausschließlich darauf ab, nur unmittelbar einzelnen Menschen zur Achtung ihrer Privatsphäre durch Organisationen zu verhelfen. Entsprechend der These von der „sozialen Konstruktion von Privatheit"[22] müssen zunächst bestimmte gesellschaftliche Verhältnisse vorliegen, die die Inanspruchnahme der „informationellen Selbstbestimmung" tatsächlich erlauben. In dieser Perspektive muss Datenschutz letztlich darauf hinwirken, dass Marktverhältnisse, Gewaltenteilung und freie Diskurse vorherrschen, weil diese den Menschen „informationelle Selbstbestimmung" nicht nur erlauben, sondern, mehr noch: von den Menschen abfordern. Wenn Personen sich nicht für ihre informationelle Selbstbestimmung interessieren und in eine offensichtlich Grundrechte missachtende Fremdbestimmung durch private Unternehmen einwilligen, dann mag das im persönlichen Einzelfall tolerierbar sein. Die Tatsache aber, dass ein Unternehmen derart agieren kann, ist ein Indikator dafür, dass sowohl der Markt als auch das Recht als auch die aufsichtsbehördliche Tätigkeit versagen.

5 Regelungsalternativen

Die Einwilligung kann dort eine Rolle spielen, wo tatsächlich Freiwilligkeit, Entkopplung von Vertrag und Einwilligung, Transparenz, vertrauenswürdige Auditierungen in Bezug auf Datenschutzkonformität sowie ein tatsächlich funktionierender Markt, ein Funktionieren des Rechtssystems[23] sowie eine funk-

21 Vgl. Rost, „Standardisierte Datenschutzmodellierung", DuD, Heft 6, 433-438.

22 Siehe Beitrag von Rost in diesem Heft.

23 Zur Problematik der Grundrechtskontrolle durch den EuGH und zum Rechtsschutz unter der EU-Datenschutz-Grundverordnung siehe: Hornung, „Eine Datenschutz-Grundverordnung für Europa? – Licht und Schatten im Kommissionsentwurf vom 25.1.2012", ZD 2012, 99-106.

tionierende Aufsichtstätigkeit vorliegen. Die Einwilligung ist insbesondere für solche Konstellationen geeignet, in denen sich Organisationen und Personen auf Augenhöhe befinden.

Als Rechtsgrundlage für die vertragliche Datenverarbeitung ist die Einwilligung durchweg ungeeignet und überflüssig. Hier sieht das Gesetz bereits jetzt eine eigene Rechtsgrundlage vor. Auch in den Fällen, in denen besondere Arten personenbezogener Daten zur Vertragserfüllung verarbeitet werden müssen, wie z. B. in der Versicherungswirtschaft, muss es eine gesetzliche Grundlage für die Datenverarbeitung geben. Hier ist der Gesetzgeber seit Jahren gefragt.[24] Mit der Einwilligung ist in diesen Fällen nichts gewonnen, denn sie entfaltet keinen Entscheidungsvorrang und keine zusätzliche Schutzwirkung: Der Vertrag kann bei Ablehnung der Einwilligung nicht zustande kommen, da es an der Grundlage für die Datenverarbeitung fehlt. Dasselbe Recht, d. h. sich für oder gegen den Vertrag zu entscheiden, haben die Betroffenen aber auch dann, wenn die Verarbeitung auf gesetzlicher Grundlage geregelt wird. Für besondere datenschutzrechtliche Risiken bei der vertraglichen Datenverarbeitung, etwa die Datenerhebung bei Dritten, wie z. B. im Versicherungsbereich, müssen spezielle Sicherungsmechanismen greifen, die dem Betroffenen Zustimmungs- und Mitwirkungsmöglichkeiten eröffnen.

Die Alternative zur Einwilligung liegt in Form gesetzlicher Regelungen auf der Hand. Immer wenn ein Allgemeinbezug der Datenverarbeitung von Organisationen besteht, dann stellt sich ohnehin die Frage nach einer gesetzlichen Regelung. Es machte schlicht ökonomisch keinen Sinn, viele Milliarden Einzelverträge zu schließen, wenn eine verallgemeinerungsfähige, vernünftige Lösung mit wenigen gesetzlichen Bestimmungen erreicht werden kann.

Das Zustandekommen von gesetzlichen Regelungen ist allerdings langwierig und würde dem gegenwärtigen Innovationstempo in Wirtschaft und Technik vermutlich nicht gerecht werden. Deswegen sollte das Instrument der Genehmigung von komplexen, personenbezogenen Verfahren erwogen werden. Anders als die bloße Pflicht zur Anzeige von Verfahren würde die Genehmigung erst nach Positiv-Prüfung durch die Aufsichtsbehörde erteilt.

Genehmigungsverfahren sind dem BDSG nicht vollkommen fremd, insbesondere dort nicht, wo besondere Gefährdungslagen für die Rechte der Betroffenen bestehen. So sieht § 4c Abs. 2 BDSG die Genehmigung von Datenübermittlungen in Staaten ohne angemessenes Datenschutzniveau vor. Nach § 38a Abs. 2 können Verhaltensregeln von Vereinigungen, die Gruppen von verantwortlichen Stellen vertreten, auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht überprüft werden. Da in diesen Fällen ein datenschutzrechtlicher Mehrwert gefordert wird, der u. a. darin liegt, dass die Datenschutzregeln für die branchentypischen Datenflüsse konkretisiert werden,[25] kommt diese Form der Anerkennung einer Genehmigung von Verfahren nahe. Im Übrigen enthält der Entwurf der Datenschutz-Grundverordnung Regelungen zur Genehmigung durch die Datenschutzaufsichtsbehörde (Artikel 34 und 42).

Bei Genehmigungsverfahren zur Verarbeitung personenbezogener Daten ließen sich insofern zwei Typen unterscheiden: Genehmigungsverfahren für Selbstregulationsvereinbarungen in Form von Codes of Conducts (a) sowie reguläre Genehmigungsverfahren (b). Anhaltspunkte für die Erforderlichkeit einer Genehmigung nach (b) sollten die hier problematisierten Datenschutzrisiken sein: Ungleichgewicht zwischen der Position des Betroffenen und der Organisation, intransparente, komplexe Verfahrensgestaltungen, große Anzahl von Betroffen, keine Möglichkeit der Nutzung von Pseudonymen.

Eine Anforderung an ein Genehmigungsverfahren wäre, dass es eindeutig schneller als ein Gesetzgebungsverfahren funktionieren muss. Dazu wären drei Aspekte zu regeln:

- Das Antragsverfahren ließe sich zweistufig anlegen: Der Antragsteller könnte verpflichtet werden, mit dem Antrag eine den Anforderungen der Datenschutzaufsichtsbehörden genügende Dokumentation, d. h. ein Datenschutzaudit oder Privacy-Impact-Assessment sowie eine vollständige Dokumentation des Verfahrens mit Datenschutzmanagementkonzept vorzulegen.[26] Daran anknüpfend könnten die Aufsichtsbehörden mit der Genehmigungsprüfung beginnen.
- Die personelle Ausstattung der Datenschutzaufsichtsbehörden muss quantitativ und qualitativ aufgestockt werden. Die Genehmigungsprüfung geschieht kostenpflichtig.
- Darüber hinaus wäre auch folgende Regelung denkbar: Eine verantwortliche Stelle dürfte ein Verfahren mit Personenbezug einsetzen, sofern sie die erforderliche Dokumentation mit dem Antrag vorgelegt, die zuständige Aufsichtsbehörde aber innerhalb von drei Monaten nicht reagiert hat. Das Verfahren gälte nach Ablauf der Frist dadurch aber nicht im Sinne einer „Genehmigungsfiktion" als genehmigt. Stellt sich heraus, dass das Verfahren rechtswidrig ist, ließe es sich immer noch nach § 38 BDSG verbieten. Dass das Verfahren ohne Genehmigung läuft, muss von der verantwortlichen Stelle kommuniziert werden. Dadurch entsteht ein Rechtfertigungsdruck auf die Tätigkeiten der Aufsichtsbehörden, der wiederum an die Politik weitergegeben werden kann.

6 Fazit

Wenn insbesondere Privatorganisationen so mächtig werden, dass sie es sich weitgehend folgenlos leisten können, Datenschutzanforderungen zu ignorieren, dann hat das gesamtgesellschaftliche Folgen. Hier kommen wir mit dem Konzept der Einwilligung, das ausschließlich auf den Schutz des Einzelnen gerichtet ist, nicht weiter. Das Thema gewinnt eine weitere Dimension, wenn man zusätzlich berücksichtigt, dass der Staat mehr und mehr Befugnisse erhält, um auf die umfangreichen Datensammlungen der Privaten zugreifen zu können.

Die folgenlosen Rechtsbrüche, die durch die Praxis nicht-rechtskonformer Einwilligungen vorliegen, sind gültige Indikatoren dafür, dass weder Markt noch Gewaltenteilung noch die Rechtsdurchsetzung tatsächlich funktionieren. Deren Funktionieren ist jedoch eine notwendige Voraussetzung dafür, dass informationelle Selbstbestimmung mehr ist als nur eine juristische Fiktion.

24 In der Diskussion wird zumeist darauf verwiesen, dass die Datenschutz-Richtlinie 95/46/EG einer gesetzlichen Grundlage entgegensteht. Leider wurde auch im Entwurf der Datenschutz-Grundverordnung bisher versäumt, eine entsprechende Regelung vorzusehen.

25 Vgl. Petri in: Simitis (Hrsg.), BDSG, § 38a Rn. 17.

26 Vgl.Rost/Bock, „Impact Assessment im Lichte des Standard-Datenschutzmodells", DuD, Heft 2012/ 06, 472-477.