Von der Formalisierung zum Desinteresse – ein „Teufelskreis“

Die Anfänge des Datenschutzes in Deutschland waren stark geprägt von den sich rasch entwickelnden technischen Möglichkeiten in der Datenverarbeitung. Vor allem spielte in der Entwicklung des Datenschutzes zunächst der Schutz des Bürgers vor unkontrollierbaren technischen Möglichkeiten und nicht legitimierter staatlicher Macht oder Gefahren durch Machtinteressen eine große Rolle.

Auch das Volkszählungsurteil des Bundesverfassungsgerichtes Mitte der achtziger Jahre stärkte den Schutz des Einzelnen und prägte den bis heute maßgeblichen Begriff vom „Recht auf informationelle Selbstbestimmung“. Der Einzelne, der Bürger, sollte grundsätzlich selber darüber entscheiden können, welche Stellen was und zu welchem Zweck über ihn wissen. Aus dieser Zeit stammt auch noch der Satz „Meine Daten müsst ihr raten“.

Im Laufe der Jahre hat sich dies geändert. Heute sind es vor allem wirtschaftliche Aspekte, die den Zugriff auf personenbezogene Daten interessant machen. Nach drei Jahrzehnten ist mittlerweile das Objekt des Datenschutzes (der Datenbesitzer, juristisch der Betroffene) offenbar der gegenwärtigen Realität abhandengekommen. Von einigen auch in den Medien beachteten Datenschutzvorfällen abgesehen, scheint sich der Einzelne, der Bürger nicht mehr so recht um den Schutz seiner Daten zu kümmern. Eine kritische Auseinandersetzung mit unkontrollierbaren technischen Möglichkeiten findet sich nur in vergleichsweise geringem Umfang. Das Internet wird genutzt, bereitwillig Daten preisgegeben und verschickt. Dabei tummeln sich gleich Heerschaaren von Dateninteressenten im Netz, die diese Daten gern für ihre Zwecke verwenden möchten und dies auch häufig tun. Hier einige Beispiele für Datenerhebungen, wie sie heute gang und gäbe sind:

- Videoüberwachung findet an vielen Stellen statt.
- Handydaten lassen nicht nur die Überwachung des Kommunikationsverhaltens zu, es entstehen auch Bewegungsprofile.
- Per GPS lassen sich auch die Nutzer orten.
- Auch am Arbeitsplatz hinterlässt der Bürger/Beschäftigte so manche Information.
- Google, Facebook und Co. Sammeln alle möglichen Daten über das Surf-Verhalten und verwerten sie.

Die Liste ließe sich mit unterschiedlichen Schwerpunkten beliebig verlängern. Was für den Verlust der kritischen Auseinandersetzung mit technischen Gefährdungspotentialen gilt, fin-

det sich auch im Umgang mit den, in der letzten Zeit teilweise hektischen, gesetzgeberischen Maßnahmen. Fakt dabei: Immer mehr wird der (Daten-) Schutz des Einzelnen den meist nicht näher definierten „Schutzinteressen“ der Allgemeinheit unterstellt.

Alles wird gesetzlich geregelt. Hier spielt auch die Gesetzgebung zur inneren Sicherheit eine bedenkliche Rolle. Dabei greift der Staat in immer stärkerem Maße auf persönliche bzw. personenbezogene Daten zu:

- Die Mautstationen an den Autobahnen erlauben eine lückenlose Überwachung der vorbeifahrenden Fahrzeuge.
- Der Zahlungsverkehr wird überwacht.
- Das Bankgeheimnis ist größtenteils aufgehoben.
- Fluggastdaten werden weltweit an die Sicherheitsbehörden geliefert.
- Vom Säugling bis zur Greisin hat jeder Bürger eine lebenslange Steuernummer. Die auch nach Ansicht des Bundesdatenschutzbeauftragten Peter Schaar schleichend für immer mehr Bereiche Anwendung findet.
- Auch die Diskussion zur Vorratsdatenspeicherung bei den Telekommunikationsverbindungsdaten lebt trotz des Urteils durch das Bundesverfassungsgericht weiter und feiert fröhliche Urständ.
- Der durchsichtige Bürger wird zumindest am Flughafen durch Nacktscanner Wirklichkeit.

Eine breite Diskussion um die häufig individualrechtlich einschränkenden gesetzlichen Maßnahmen findet kaum oder selten statt. Die Mehrheit der betroffenen Bürger scheint sich gar nicht mehr darum kümmern zu wollen.

Warum ist das so?
Abgesehen davon, dass eine komplexe Technologie auf kompliziertes Recht stößt, es also doppelten Grund für Unverständnis gibt oder geben kann, existieren wichtige Gründe, warum Datenschutz so schwer fassbar ist.

1. Wir alle unterschätzen abstrakte Risiken. Wer Information über sich weitergibt, kann nicht einschätzen was mit ihnen passieren wird und welches Risiko er ggf. mit der Weitergabe eingeht.
2. Da Daten in der Regel maschinell verarbeitet werden, gibt es auch unzählige Möglichkeiten sie aus ihrem Zusammenhang zu reißen und sie neu zu verknüpfen (Ein kritisches Thema wäre Datenschutz in Datenbanken). Dies lässt ein neues realitätsfernes Bild entstehen.
3. Daten lassen sich nicht mit unserem üblichen Eigentumsbegriff fassen. Wir können unsere Daten einem Anderen geben und sie trotzdem behalten. Aus diesem Grund geben viele Bürger ihre Daten schon für die Chance vermeintlicher Vorteile weiter (Rabattsysteme, Preisaufschreiben, freie Mailaccounts und Ablage von Daten bei Providern (Bilder, Texte, Musik).

Zu dieser Entwicklung passt, dass viele Profis im Datenschutz die Abbildung der Belange der Betroffenen lediglich juristisch geregelt sehen. Für Juristen sicher ein interessantes Arbeitsfeld. Dabei fällt das Thema technisch-organisatorische Maßnahmen zur Gewährleistung von Betroffenenrechten hinter die juristische Ausgestaltung zurück. Da die Proteste der Objekte des Datenschutzes, die betroffenen Bürger, offensichtlich verstummt sind, scheinen sich deren Belange doch auch gut formal rechtlich regeln zu lassen.

Wie wird der Datenschutz rechtlich umgesetzt?

Der Datenschutz steht hier immer vor dem Dilemma, Grundrechte gegeneinander abwägen zu müssen. Auf der einen Seite stehen meist die berechtigten wirtschaftlichen Interessen von Unternehmen und auf der anderen Seite der Schutz der Persönlichkeitsrechte der Bürger. Dies wird mit dem juristischen Werkzeug der Interessenabwägung umgesetzt. Hierzu Prof. Simitis:

„Das BDSG entscheidet sich zwar für eine Interessenabwägung, lässt aber bei den Abwägungsmaßstäben jede Präzision vermissen. Schon die „berechtigten Interessen“ sind schwer zu definieren. Fast noch schwieriger ist es, die „schutzwürdigen Interessen“ einigermaßen verlässlich zu umschreiben. Der Gesetzgeber ist in Wirklichkeit jedem Versuch aus dem Weg gegangen, klare Anhaltspunkte zu formulieren, und hat sich statt dessen darauf beschränkt, eine bereits im BDSG 77 verwendete, letztlich nichtssagende Generalklausel zu wiederholen.“ (Simitis in SIMITIS, 7 Auflage, §28 RN 126)

Zusätzlich wird der Begriff des schutzwürdigen Interesses im BDSG dann auch noch in unterschiedliche Zusammenhänge gesetzt.

1. *... soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das* ***schutzwürdige Interesse*** *des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung* ***überwiegt.*** *(§ 28, Abs. 1 Nr. 2)*
2. *... 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)*
3. *Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit* ***schutzwürdige Interessen*** *des Betroffenen* ***nicht entgegenstehen****.*
   (§ 28, Abs. 3, Satz 6)

Wird der Datenschutz rein aus juristischer Sicht betrachtet, so wird er schlussendlich zur Domäne einiger weniger Spezialisten. Weder der betroffene Bürger selbst, noch der Verantwortliche in einer verarbeitenden Stelle, können hier ohne Spezialisten die Rechtmäßigkeit der Datenverarbeitung bewerten. Hier ist die Frustration am Datenschutz vorprogrammiert. In vielen Bereichen entzieht sich der Datenschutz so einer praktischen Anwendung, da de Facto kein Bürger angesichts der unklaren Rechtlage die Situation einschätzen bzw. seine Rechte durchsetzen kann. So verbleibt die Deutungshoheit über den Rahmen der „zulässigen“ Datenverarbeitung bei den verantwortlichen Stellen, also den Datennutzern. Zwar ist auch für sie die Rechtslage oftmals unklar, trotzdem haben sie, frei nach Jellinek, die „normative Kraft des Faktischen“ auf ihrer Seite und bestimmen so den Alltag im Datenschutz.

Ein anderes Beispiel für die Probleme, die die rechtliche Umsetzung des Datenschutzes bereitet, ist die Ausklammerung moderner Unternehmensstrukturen aus dem Bundesdatenschutzgesetz. In der wirtschaftlichen Realität spielen Organisationsstrukturen, vor allem Konzerne, eine wichtige Rolle. Im Datenschutz werden derartige Strukturen nicht berücksichtigt. Jede einzelne Tochtergesellschaft wird als alleinige, selbstständige in sich geschlossene Einheit im Datenschutz betrachtet. Obwohl es gute Gründe für eine derartige Regelung gibt, führt sie zu weiteren Unklarheiten, da sich wirtschaftliche Realität und Datenschutzrealität nicht decken. Im Falle der Datenverarbeitung im Auftrag kontrolliert häufig die Konzerntochter als verant-

wortliche Stelle die Konzernmutter, sofern sie als Auftragnehmer fungiert. So ist der Datenschutzalltag im Konzern von Workarounds und Ersatzkonstruktionen zur Herstellung einer rechtlich halbwegs soliden Grundlage für die Datenverarbeitung geprägt. Dieser Zustand ist für die Akzeptanz des Datenschutzes in der Konzernführung, besonders bei ausländischen Konzernmüttern, nicht gerade förderlich.

Es fehlen offensichtlich geeignete Methoden, den Datenschutz effektiv und praxisnah umzusetzen. Dies betrifft natürlich nicht nur Wirtschaftsunternehmen, sondern auch gesetzgeberische Maßnahmen in diesem Bereich. Es wird versucht den technischen, politischen und gesellschaftlichen Anforderungen durch ein immer komplizierter werdendes juristisches Regelwerk gerecht zu werden. Einer Weiterentwicklung, in Anbetracht der dargestellten gesellschaftlich notwendigen Ausgestaltung von Betroffenen- oder Bürgerrechten, mit entsprechender Verantwortung, wird hier mehr und mehr der Raum entzogen. Es kommt zum **Circulus vitiosus** (Teufelskreis). Die schleichende Formalisierung des Datenschutzes bewirkt eine immer größere Unübersichtlichkeit, der Einzelne sieht sich immer weniger in der Lage die Situation zu beurteilen. Dies bedingt im Effekt ein immer stärkeres Desinteresse bei denjenigen, um deren Daten und Rechte es geht, den Betroffenen, den Bürgern. Die daraus resultierende „Abwesenheit“ des mündigen Bürgers lassen die oben geschilderten formalen Lösungen immer mehr als ein probates Mittel des Datenschutzes erscheinen. Andere Lösungsansätze sind daher scheinbar unnötig.

Was ist zu tun?

Beispielsweise im jetzigen Datenschutzgesetz des Landes Schleswig-Holstein gibt es bereits zukunftsweisende Ansätze. So finden wir unter § 4 Datenvermeidung und Datensparsamkeit, Datenschutzaudit, Abs. 2 folgende Formulierung:

„Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Verordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.“

Was spräche dagegen, Regelungen in Gesetze aufzunehmen, die konkrete Lösungen für datenschutzfreundliche Techniken beschreiben bzw. einfordern? So ist in der geplanten Novelle zum Arbeitnehmerdatenschutz zwar eine Einzelfallregelung für die Erhebung biometrischer

Verfahren geplant, leider unterlässt es der Gesetzgeber aber konkrete Vorgaben für die technische Ausgestaltung zu geben. Beispielsweise „Biometric Template Protektion“, bei diesem Verfahren werden die eigentlichen biometrischen Daten nicht gespeichert, sondern nur ein Hash-Wert, der eine Rekonstruktion des biometrischen Merkmals (z.B. Fingerabdruck) nicht zulässt, aber bei der Erkennung genauso zuverlässig ist, wie das Original.

Noch einen Schritt weiter würde der folgende Vorschlag gehen: Der Gesetzgeber verpflichtet die verantwortlichen Stellen immer dort, wo es möglich ist, den Betroffenen zusätzliche Schutzmaßnahmen anzubieten. Dies hätte den positiven Effekt, dass der Betroffene selber für seinen Datenschutz sorgen könnte und somit für den Schutz seiner Daten Instrumente bekäme. Dies würde dem zurzeit herrschenden Ohnmachtsgefühl sicher entgegenwirken.

Die hier skizzierten Lösungsansätze sind prinzipiell nichts Neues. Bereits vor 10 Jahren gab es im Gutachten „Modernisierung des Datenschutzrechts“ von Roßnagel, Garska, Pfitzmann die folgende Feststellung: *„Datenschutzrecht muss versuchen, die Entwicklung von Verfahren und die Gestaltung von Hard- und Software am Ziel des Datenschutzes auszurichten und die Diffusion und Nutzung datenschutzgerechter oder -fördernder Technik zu fördern.*“(Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka, „Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, S. 35) Weiter heißt es auf der nächsten Seite:

„Technischer Datenschutz ist auch viel effektiver als rein rechtlicher Datenschutz. Was technisch verhindert wird oder unterbunden werden kann oder einfach technisch nicht möglich ist, muss nicht mehr verboten und überwacht werden. Auch wenn die Datenverarbeitung für den Einzelnen nicht mehr vorhersehbar und überschaubar ist, wirkt technisch realisierter Datenschutz auch unabhängig vom individuellen Problembewusstsein und der persönlichen Aufmerksamkeitskapazität. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen eines Techniksystems nicht.“

Offenbar sind diese längst bekannten Methoden und Instrumente wieder in Vergessenheit geraten. Exemplarisch lässt sich bei dieser Herangehensweise zeigen, dass ein erfolgreicher und nachvollziehbarer Datenschutz nur zu erreichen ist, wenn die drei wichtigsten Komponenten auch angewendet werden, nämlich:

- Technischer Datenschutz
- Organisatorischer Datenschutz

- Rechtlicher Datenschutz

Die Fokussierung auf nur eine Komponente ist zum Scheitern verurteilt. Hier ist eine interdisziplinäre Zusammenarbeit erforderlich.

Dies ist der Ansatz der Grid eg, auf deren Seiten solche und ähnliche Diskussionsthemen zukünftig zur Verfügung stehen sollen. Die Grid eg bringt Experten aller drei Fachrichtungen zusammen. Dem Grundsatz folgend, dass komplexe Probleme wie der Datenschutz immer die Expertise diverser Fachleute erfordern.

Die Grid eg möchte die Diskussion neu eröffnen. Es wäre Zeit für eine „neue Aufklärung“ im Datenschutz, die diskutiert, was sich da in der Zwischenzeit seit dem Volkszählungsurteil getan hat. Allerdings wäre dies auch eine wichtige Aufgabe für Datenschutzprofis, die einiges über den gesetzlichen Aufgabenkatalog hinausginge, ohne diesen natürlich zu negieren.

Für solche Diskussionen stehen durchaus Information zur Verfügung. Nicht nur einige Aufsichtbehörden und Datenschutzorganisationen haben sehr gute Webseiten auf denen viele Hintergrundinformationen und praktische Hilfen verfügbar sind. Dafür gibt es auch eine Reihe von Verlagen und Institutionen, die teilweise online und aktuell Informationen bereitstellen. Auch die Datenschutzprofis können dabei helfen, Informationsquellen konstruktiv zu nutzen und zu erschließen.

Autoren: Jochen Brandt, Dr. Andreas Höpken
Grid eG
Eckerkoppel 89
22159 Hamburg
email: info@grideg.de
Internet: www.grideg.de