# Datenschutz auf dem Weg in den Cyberspace

David Gill, LL.M.

Berliner Beauftragter für Datenschutz und Informationsfreiheit
Pallasstraße 25/26
10781 Berlin
gill@datenschutz-berlin.de

**Abstract:** Es werden Themenschwerpunkte der gegenwärtigen Modernisierungsdebatte zum Datenschutzrecht dargestellt, mit denen sowohl auf die Entwicklung der Datenverarbeitungstechnik als auch auf den gestiegenen wirtschaftlichen Wert von Informationen reagiert werden soll. Grundlage ist ein Gutachten zur Modernisierung des Datenschutzrechts, das im Jahr 2001 im Auftrag des Bundesministeriums des Innern erstellt wurde.[1]

Als das Datenschutzrecht vor einem viertel Jahrhundert in Deutschland laufen lernte, war die Welt noch in Ordnung. Die zu schützenden personenbezogenen Daten waren auf Papier oder in Großrechnern, an deren Vernetzung im großen Stil nicht zu denken war, gespeichert. Zur Erhebung zusätzlicher Daten musste man die Betroffenen selbst oder Dritte befragen oder in den physischen Besitz von Papieren, auf denen diese aufgeschrieben waren, gelangen und hernach die erlangten Daten auf ein Blatt Papier schreiben oder per Tastatur in einen konkreten Rechner einspeisen. Die Bedrohung vor der es vor allem zu schützen galt, waren staatliche Großrechner.[2] Kurzum, Datenschutz war ein geradezu überschaubares Feld.

Dies hat sich geändert. Datenverarbeitung findet überall statt, im Büro, zu Hause oder auch auf der Straße. Noch nie war es so leicht und auch so billig, Daten zu erheben und zu speichern. Durch die Vernetzung sind heute Daten in einem schier endlosen Umfang zugänglich – offen durch Suchmaschinen auffindbar, aber auch mit den notwendigen technischen Kenntnissen ohne Zustimmung oder gar Kenntnis der Besitzer. Jeder PC-Besitzer verfügt heute über Speicherkapazitäten, die einem großen Archiv von vor fünfzig Jahren entsprechen. Speicherkapazitäten sind überdies kaum mehr eine Frage des Geldes oder gar der räumlichen Kapazitäten, die früher für Großrechner eine Rolle spielten. Dies verleitet dazu, Daten für den Fall der Fälle, unabhängig vom Zweck der Erhebung und einer künftigen Nutzung auch auf Vorrat zu speichern, nach dem Motto: Wer weiß, wozu ich die noch brauchen könnte. Die Leistungsfähigkeit der Kommunikationsnetze fördert die Möglichkeiten, Daten über eine Person aus verschiedenen Lebensbereichen zusammenzutragen und daraus ein dezidiertes Persönlichkeitsprofil des Betroffenen zu erstellen. Der Marktwert der Daten steigt, denn je mehr man über einen potentiellen Kunden weiß, umso besser kann der „Angriff“ auf den Geldbeutel des Verbrauchers

[1] [RPG01]
[2] [RPG01] S. 22

geplant werden. Die Vernetzung von Alltagsgegenständen wie Handy, Kühlschrank oder Bordcomputer im Auto (Ubiquitous Computing) liefert darüber hinaus eine Unmenge weiterer Daten über ihre Nutzer.

Vor diesem Hintergrund ist es offensichtlich, dass das Konzept, alle nur erdenklichen Datenverarbeitungskonstellationen gesetzlich regeln zu können, angesichts der Komplexität der Materie wie auch der dynamischen Entwicklung der technischen Möglichkeiten, denen mit einer langwierigen Gesetzgebungspraxis nur unzureichend begegnet werden kann, nicht der Weisheit letzter Schluss ist. Daher muss ein künftiges Datenschutzrecht neue Wege beschreiten und zusätzliche Mechanismen schaffen, die es den Akteuren selbst in Ergänzung zu und Konkretisierung von gesetzlichen Vorgaben ermöglicht, Maßnahmen zum Schutz personenbezogener Daten selbst zu initiieren und verbindliche Regelungen zu entwickeln. Stichworte sind hier Selbstdatenschutz der Betroffenen und Selbstregulierung durch die Datenverarbeiter. Aufgabe des Gesetzgebers muss es dabei insbesondere sein, für ein ausgewogenes Verhältnis zwischen beiden zu sorgen.[3] Dies gilt gleichermaßen für die Offline- wie die Online-Welt und soll anhand ausgewählter Vorschläge, die in der Diskussion um die Modernisierung des Datenschutzrechts eine Rolle spielen, dargestellt werden.

Am besten werden Daten geschützt, wenn sie weder erhoben noch weiter verarbeitet werden. Dieser Grundsatz der **Datensparsamkeit und Datenvermeidung** hat den gesamten Datenverarbeitungsprozess im Auge. So wie ein wirtschaftlich denkender Mensch seine finanziellen Aufwendungen in der Regel möglichst gering halten möchte, also sparsam wirtschaftet, soll es auch im Rahmen der Datenverarbeitung eine Selbstverständlichkeit werden, personenbezogene Daten nur in dem Umfang zu nutzen, wie dies tatsächlich erforderlich ist. Eine Überprüfung, ob die Verarbeitung personenbezogener Daten tatsächlich für die Zweckerreichung erforderlich ist, hat unter diesem Vorzeichen in zweifacher Hinsicht zu erfolgen:[4] In einem ersten Schritt stellt sich die Frage, ob das konkrete Datum für den Zweck der Datenverarbeitung und den dazu notwendigen Prozesse erforderlich, seine Nutzung also unverzichtbar ist. Dies kann nicht abstrakt erfolgen, sondern muss für jede einzelne Phase der Datenverarbeitung (Erhebung, Speicherung, Übermittlung etc.) festgestellt und berücksichtigt werden. Aus letzterem ergibt sich auch, wann ein Personenbezug gelöscht werden kann und muss. Wurde in diesem ersten Schritt festgestellt, dass die Daten für den konkreten Zweck verarbeitet werden müssen, ist nunmehr zu prüfen, ob dies auch in anonymisierter oder ggf. pseudonymisierter Form ausreichend ist, da ein Personenbezug nicht notwendig ist.

Mit dem Grundsatz der Datenvermeidung und Datensparsamkeit korrespondiert der **Systemdatenschutz**, der die konzeptionellen Festlegungen zur Datenverarbeitung im Einzelfall in verfahrensimmanente organisatorische und technische Vorkehrungen umsetzt. Unter Systemdatenschutz versteht man alle diejenigen Maßnahmen, die dafür sorgen, dass ein konkretes Verfahren und die dabei genutzte Technik nur in dem Umfang zur Datenverarbeitung imstande ist, zu dem es rechtlich, beispielsweise aufgrund einer

[3] vgl. [Wt01], S. 265.
[4] [RPG01], S 101 f.

Einwilligung des oder eines Vertragsverhältnisses mit dem Betroffenen oder aufgrund eines Gesetzes, befugt ist.[5] Eine wichtige Rolle hierbei spielt die Entwicklung und Einführung datenschutzfördernder Technik (Privacy Enhancing Technologies), die beispielsweise eine datensparsame Übermittlung oder die Abschottung verschiedener Verarbeitungsbereiche ermöglicht. Staatliche Maßnahmen, bis hin zu einer Bevorzugung in der Beschaffung durch öffentliche Stellen, sollten diese fördern.[6]

**Transparenz** der Datenverarbeitung gegenüber der betroffenen Person setzt zum einen ihre Kenntnis von der Tatsache voraus, dass ihre Daten verarbeitet werden, zum anderen, wie und zu welchem Zweck dies geschieht. Das Bundesverfassungsgericht hat mit der Formel „wer was wann bei welcher Gelegenheit über sie weiß" diese Grundvoraussetzung der informationellen Selbstbestimmung der Bürger beschrieben.[7]
Kenntnis erhält sie dadurch, dass die Daten offen bei ihr erhoben werden, sie also um Mitteilung der entsprechenden Daten gebeten wird. Dieser Grundsatz der Erhebung beim Betroffenen ist nicht neu (§ 4 Abs. 2 Satz 1 BDSG). Doch auch eine Erhebung bei Dritten kann wegen des Zwecks der Datenerhebung notwendig sein, setzt allerdings eine gesetzliche Grundlage oder einen legitimen Verarbeitungszweck voraus, der gesetzlich fest umrissen sein muss. Allerdings muss auch sie grundsätzlich mit einer Unterrichtung der Betroffenen einhergehen, wie dies bereits im TDG oder MDStV vorgesehen ist.
Die alleinige Information darüber, dass eine Datenverarbeitung stattfindet reicht aber bei weitem nicht aus. So ist es eine Selbstverständlichkeit, dass die Unterrichtung über die Datenverarbeitung die Angaben nach § 4 Abs. 3 BDSG zur datenverarbeitenden Stelle und zum Zweck der Datenverarbeitung sowohl für die Erhebung bei den Betroffenen als auch bei Dritten enthält. Um nicht Objekt sondern Subjekt der Datenverarbeitung zu sein, muss der Betroffene überdies Kenntnis von der Struktur und Funktionsweise der entsprechenden Datenverarbeitungsverfahren und –systeme („Was tut die Maschine mit meinen Daten?"), von technischen und organisatorischen Maßnahmen, die dem Datenschutz und der Datensicherung dienen, von den gesetzlichen Grundlagen und anzuwenden Verhaltensregeln der Datenverarbeiter und von Beschwerdeverfahren im Falle eines Verstoßes gegen Datenschutzbestimmungen nehmen können.[8] Für die Transparenz der Datenverarbeitung entscheidend wird es auch sein, inwieweit die Forderung nach einer Offenlegung der Quellen der verwendeten Software-Produkte („open source") und damit einer Nachvollziehbarkeit der Verfahrensabläufe berücksichtigt wird.

Mit § 38 a BDSG hat der Gesetzgeber erstmals Berufsverbänden und anderen Vereinigungen von datenverarbeitenden Stellen die Möglichkeit eröffnet, Regelungen zur Förderung und Durchführung datenschutzrechtlicher Regelungen aufzustellen. Diese **Selbstregulierung** als Element des Datenschutzes gilt es auszubauen.[9] Um eines aber gleich klarzustellen: Die Betroffenen sollen damit nicht zum Spielball der Datenverarbeiter gemacht werden, vielmehr wird die Selbstregulierung nur im Rahmen allgemeiner gesetzlicher Vorgaben bewegen können, für die angesichts des

[5] vgl. [RPG01], S. 39 f.
[6] [RPG01], S. 147 f.
[7] BVerfGE 65, 1 (43).
[8] [RPG01], S. 86 f.
[9] ausführlich hierzu: [RPG01], S. 153 ff.

gesetzlicher Vorgaben bewegen können, für die angesichts des verfassungsrechtlichen Schutzgebotes der informationellen Selbstbestimmung der Gesetzgeber auch weiterhin in der Pflicht ist. Überdies werden solche Verhaltensregeln nur dann sowohl für diejenigen, die sie aufstellen, wie auch für die Kontrollstellen verbindlich sein können, wenn sie durch eben diese Aufsichtsbehörde auf ihre Vereinbarkeit mit gesetzlichen Vorgaben überprüft und hernach rechtlich anerkannt werden.

Die Chancen einer solchen „regulierten Selbstregulierung“ und ihre Vorteile für die Beteiligten sind vielfältig und gehen angesichts ihrer Verbindlichkeit für Datenverarbeiter und Aufsichtsbehörden über bisherige „codes of conduct“ oder Datenschutzerklärungen von Unternehmen, auf deren Erstellung und ggf. Änderung andere keinen Einfluss haben, hinaus:

Verhaltensregeln können sich anders als abstrakte Gesetze an der Datenverarbeitungspraxis orientieren und somit branchen- oder unternehmensbezogenen Besonderheiten Rechnung tragen. Im Gegensatz zu einem Gesetz, das ein langwieriges Verfahren durchlaufen muss, können sie schnell auf technische Entwicklungen reagieren und sowohl deren Gefahren für die Persönlichkeitsrechte der Betroffenen als auch deren Potenziale für die Förderung des Datenschutzes berücksichtigen. Sie vereinheitlichen die Datenschutzpraxis für ganze Wirtschaftszweige, erleichtern es dadurch dem einzelnen Unternehmen, datenschutzgerechte Verfahrensweisen einzuführen und verschaffen den Betroffenen Übersichtlichkeit, beispielsweise durch einheitliche Einwilligungsklauseln oder Beschwerdeverfahren einer ganzen Branche. Ihre Anerkennung durch die Aufsichtsbehörden kann ein Vertrauensfaktor der Verbraucher in die sich den Regeln unterwerfenden Unternehmen sein. Die Attraktivität von Verhaltensregeln für die Wirtschaft liegt darin begründet, dass sie nach Anerkennung durch die Aufsichtsbehörden über eine verlässliche Grundlage ihrer Datenverarbeitung verfügt, die Unsicherheiten aufgrund der Auslegungshoheit der Kontrollstellen hinsichtlich abstrakter datenschutzrechtlicher Bestimmungen beseitigt. Interessant wären verbindliche Verhaltensregeln auch für den internationalen Datentransfer.

Selbstregulierung darf aber nicht als Instrument der Interessensdurchsetzung der Wirtschaft missbraucht werden. Das demokratische Defizit ihrer Erstellung wird durch ihre Anerkennung durch die Kontrollstellen minimiert. Darüber hinaus sollten auch die Betroffenen ein Mitspracherecht bei ihrer Entwicklung erhalten um eine einseitige Ausrichtung an den Interessen der Wirtschaftsverbänden zu verhindern. Verbraucher- und Datenschutzverbänden könnten als Korrektiv eingebunden werden, wie dies im übrigen auch seitens der Europäischen Union gefordert wurde.[10] Ein weiteres Regulativ muss die zeitliche Begrenzung der Anerkennung von Verhaltensregeln sein, die die Überprüfbarkeit ihrer Rechtmäßigkeit insbesondere im Hinblick auf die technische Fortentwicklungen sicherstellt.

Personenbezogene Daten sind aber auch Identifier automatisch miteinander kommunizierender Maschinen, da diese einzelnen Personen zuzuordnen sind, oder „Überschuss-

[10] Grünbuch „Informationen des öffentlichen Sektors – eine Schlüsselressource in Europa“, KOM (1998) 585, 26; s. auch [Wt01], S. 269.

daten“ bei Suchprozessen im Internet. Die beiden Beispiele haben mit weiteren gemein, dass es dem Nutzer auf den Personenbezug offensichtlich nicht ankommt, dieser vielmehr nur als Nebenprodukt eines Prozesses entsteht. Für diese **Verarbeitung ohne gezielten Personenbezug**[11] sollten daher gesonderte Regelungen entwickelt werden, die auf der einen Seite ihre Verarbeitung erleichtern, indem beispielsweise ein Auskunftsanspruch des Betroffenen nicht besteht, da dies letztlich zu einer Speicherungspflicht dieser nicht länger benötigten Daten führen würde, sie auf der anderen Seite aber einer strengen Zweckbindung und sofortigen Löschungspflicht unterwirft.

Schließlich sollte auch das rechtliche Grundverständnis, das sich im deutschen Datenschutzrecht widerspiegelt, überdacht werden. So gehen die deutschen Datenschutzgesetze vom Grundsatz des **Verbots mit Erlaubnisvorbehalt** aus. Überspitzt heißt dies, dass zunächst einmal alles, was mit der Verarbeitung personenbezogener Daten zu tun hat, verboten ist, andernfalls eine Ausnahme vorliegen muss. Das heutige Datenschutzrecht versteht die Kommunikation mit dem Bürger also als Ausnahme.[12] Dieses Paradigma mag zwar auf den ersten Blick die beste Lösung für den Schutz der informationellen Selbstbestimmung sein, entspricht aber weder den tatsächlichen Gegebenheiten hinsichtlich der „Ausnahmen“ (Hunderte! von Landes- und Bundesgesetzen), noch den Kommunikationsbedürfnissen der Informationsgesellschaft. Ohne den rechtlichen Schutz der Betroffenen zu minimieren, würde ein moderner Ansatz des Datenschutzrechts daher die grundsätzliche gesetzliche Erlaubnis der Datenverarbeitung sein, soweit bei dieser präzise formulierte Grundsätze eingehalten werden. Zu diesen Grundsätzen gehören die Zulässigkeit der konkreten Datenverarbeitung, entweder aufgrund der Einwilligung des Betroffenen oder – in wenigen unbedingt erforderlichen Fällen, wie beispielsweise im Sicherheitsbereich – aufgrund einer gesetzliche Erlaubnis, die Transparenz, Erforderlichkeit und Zweckbindung sowie die Einhaltung von Vorgaben zur Datensicherung.

## Literaturverzeichnis


[Bj01] Bizer, J.: Ziele und Elemente der Modernisierung des Datenschutzrechts. DuD 2001, S. 274.

[RPG01] Roßnagel, A.; Pfitzmann, A.; Garstka, H.: Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Innern. Berlin, 2001.

[Wt01] Weichert, T.: Datenschutz als Verbraucherschutz. DuD 2001, S. 264.


[11] [RPG01], S. 68 f.

[12] [Bj01], S. 275.