Erschien in: Erwin Staudt (Hrsg): Deutschland online; Standortwettbewerb im Informationszeitalter; Projekte und Strategien für den Sprung an die Spitze; Springer-Verlag Heidelberg, 2002, Seite 89-98

Datenschutz im Internet –
Welche Standards informationeller Selbstbestimmung braucht das Internet?

Alexander Roßnagel

Universität Kassel
Fachbereich 10, Öffentliches Recht
34109 Kassel
rosnagel@hrz.uni-kassel.de

Andreas Pfitzmann

TU Dresden
Fakultät Informatik
01062 Dresden
pfitza@inf.tu-dresden.de

1 Datenschutz unter Druck

So berechtigt die Forderung nach den Anschlägen vom 11. September war, dass sich solche Mordanschläge auf Tausende unschuldiger Menschen nicht wiederholen dürfen, so ungerechtfertigt war die Behauptung, diesem Ziel stünde der Datenschutz im Weg. Bereits zuvor erlaubten die Strafprozessordnung, das erst im Sommer 2001 novellierte Gesetz zu Art. 10 GG und viele weitere Regelungen eine umfassende Überwachung der Telekommunikation. Im Herbst 2001 haben die beiden Sicherheitspakete sowie die neue Telekommunikationsüberwachungsverordnung die Befugnisse von Polizei und Geheimdiensten noch stärker erweitert. Weitere Überwachungsbefugnisse sind geplant. Im Sicherheitsbereich scheint es nicht zu viel, sondern zu wenig Datenschutz zu geben.

Datenschutz und Überwachung sind grundsätzlich miteinander vereinbar. Das Recht auf informationelle Selbstbestimmung, das durch Datenschutzmaßnahmen geschützt werden soll, ist zwar das zentrale Grundrecht der Informationsgesellschaft und die Grundlage jeder demokratischen Ordnung. Dennoch kann diese Selbstbestimmung eingeschränkt werden, wenn anders Leben und Freiheit nicht gesichert werden können. Zulässig sind gesetzliche Einschränkungen, die zur Erreichung dieses Ziels geeignet, in Reichweite und Eingriffstiefe möglichst schonend und angesichts der Größe der abzuwehrenden Gefahr für die Betroffenen

objektiv zumutbar sind.[1] Tatsächlich effektiv möglicher und erforderlicher Überwachung steht die informationelle Selbstbestimmung nicht im Weg.

Im Folgenden werden mögliche Überwachungsmaßnahmen im Internet daraufhin geprüft, ob sie für den allseits akzeptierten Zweck, Terroranschläge wie die von New York und Washington zu verhindern, geeignet und erforderlich sowie gegenüber den mit ihnen verbundenen Einschränkungen vertretbar sind (2). Daran schließen sich Überlegungen an, inwieweit die künftige Entwicklung von eCommerce und eGovernment auf einen funktionsfähigen Datenschutz im Internet angewiesen ist und wie dieser gewährleistet werden kann (3). Entscheidend wird sein, beide Aspekte zusammen zu sehen (4).

2 Überwachung im Internet

Das Ziel vieler "Bedarfsträger", wie die Polizei-, Strafverfolgungs- und Geheimdienstbehörden im Jargon des Überwachungsrechts genannt werden, ist es, alle Kommunikationsvorgänge im Internet aktuell überwachen wie auch noch nach längerer Zeit nachvollziehen zu können. Damit sollen verdeckte oder potenzielle Terroristen so frühzeitig erkannt werden, dass mögliche Anschläge verhindert werden.

Um dieses Ziel zu erreichen, haben die Bedarfsträger in der Bundesrepublik Deutschland bereits durchgesetzt, dass Internet Service Provider alle Kommunikationsvorgänge als Doppel den Bedarfsträgern anbieten müssen.

2.1 Schutz gegen Überwachung

Die Doppel, die die Bedarfsträger auswerten können, verfehlen aber ihren Sinn, wenn die Kommunikationspartner anonym bleiben oder ihre Kommunikationsinhalte verschlüsseln oder gar verstecken. Für alle drei genannten Selbstschutzmöglichkeiten gibt es seit Jahrzehnten, teilweise seit Jahrhunderten bekannte und erprobte Low-Tech-Verfahren, die weiterhin funktionieren und vermutlich immer funktionieren werden. In den vergangenen zwei Jahrzehnten wurden rechnergestützte High-Tech-Verfahren entwickelt, die alle diese Verfahren kombinieren und die Bequemlichkeit für den Nutzer steigern können bis hin zu dem Zustand, dass er ihre Benutzung überhaupt nicht mehr bewusst wahrnimmt.

---

1 S. hierzu Entscheidungen des Bundesverfassungsgerichts, Bd. 65, S. 43 ff.

Möglichkeiten der Anonymisierung der Kommunikation

Die klassische Low-Tech-Variante besteht darin, beim Kommunikationszugang anonym zu bleiben: Briefe werden ohne äußeren Absender oder mit einem unauffällig falschen äußeren Absender in den Briefkasten geworfen, öffentliche Telefone werden gegen Bezahlen mit Münzen oder mit anonym erworbenen, nur wenige Male verwendeten Wertkarten benutzt, Mobiltelefone werden anonym erworben und mit anonym oder von anderen erworbenen Pre-Paid-Karten benutzt, Internet-Cafes bieten anonymes Surfen im Internet sowie unauffälligen Zugang zu pseudonym eingerichteten E-Mail-Accounts, die sich irgendwo im Ausland befinden können. Wer den Weg ins Internet-Cafe oder eine dort mögliche Gesichtskontrolle scheut, wird sich per Telefon bei einem Internet Service Provider in einem Land ins Internet einwählen, mit dem preiswert und leistungsfähig telefoniert werden kann, aber kein Rechtshilfe- oder gar Überwachungsabkommen besteht. Die moderne rechnergestützte High-Tech-Variante besteht darin, das Netz selbst bzw. im Netz angebotene Dienste für die Anonymisierung zu nutzen: Proxies ersetzen die Absenderangabe durch ihre eigene und werden teilweise eigens für diese Pseudonymisierung betrieben.[2] Umcodierende MIXe ändern zusätzlich noch die Codierung der Nachrichten, damit auch durch Vergleich aller ein- und ausgehenden Nachrichten diese Nachrichten nicht miteinander in Beziehung gesetzt werden können. Damit dieses Umcodieren klappt, müssen die Nachrichten passend vorbereitet werden, was mittels einer auf dem PC des Benutzers installierten Software geschieht.[3]

Möglichkeiten der Verschlüsselung

Die aus Agentenromanen bekannten *Codebücher*, in denen zwischen Sender und Empfänger verabredet ist, wie Nachrichten zu verschlüsseln sind, indem Worte, Wortgruppen oder gar ganze Aussagen durch andere Worte, Wortgruppen oder Aussagen oder auch beliebige kryptische Zeichen ersetzt werden, sind die klassische low-tech Alternative bei der Verschlüsselung. Ebenfalls low-tech im Sinne von „per Hand durchführbar“ ist das *One-Time-Pad*, bei dem zur Klartextnachricht ein abschnittsweise nur einmal verwendeter (und deshalb One-Time-Pad genannter) Schlüssel hinzuaddiert wird – der Empfänger subtrahiert ihn wieder und erhält so genau die ursprüngliche Nachricht. Obwohl zumindest für kürzere Nachrichten auch ohne technische Hilfsmittel durchführbar, ist diese Verschlüsselung für diejenigen, die den Schlüsselabschnitt nicht kennen, nicht zu entschlüsseln – sie mögen so viel und so lange rechnen, wie sie können und wollen.

Nachteil dieser Low-Tech-Varianten ist, dass diejenigen, die so verschlüsselt kommunizieren wollen, einen gemeinsamen, vertraulich ausgetauschten Schlüssel

---

2 S. z.B. www.anonymizer.com.

3 S. z.B. www.onion-router.net; http://anon.inf.tu-dresden.de/.

benötigen. Der Austausch vertraulicher Schlüssel ist entweder aufwendig – oder möglicherweise doch insofern problematisch, als der Wert des Schlüssels nicht vertraulich bleibt, wenn es sich um größere offene Gruppen handelt. Kein Problem ist der Austausch geheimer Schlüssel in kleinen Gruppen oder solchen, bei denen sich die Mitglieder zumindest einmal persönlich treffen. Solch ein Treffen kann dann genutzt werden, um dem anderen einen Datenträger mit dem Schlüssel zu übergeben. Heutige Datenträger, und hierin liegt der Übergang zu High-Tech, haben solche Speicherkapazitäten und sind so klein, leicht und preiswert, dass die Methode des One-Time-Pad, die noch vor zwei Jahrzehnten Staatspräsidenten vorbehalten war (erinnert sei an das Rote Telefon), heute jedermann preiswert zur Verfügung steht.

Ein zweiter Aspekt von High-Tech ist die seit den Jahren 1976/78 bekannte *asymmetrische* Kryptographie. Bei ihr erzeugen Teilnehmer nicht einzelne Schlüssel, die sie wie in der obigen Beschreibung vertraulich austauschen, wonach beide Teilnehmer die gleiche Schlüsselkenntnis besitzen, diesbezüglich also *symmetrisches* Wissen haben. Bei der asymmetrischen Kryptographie erzeugen Teilnehmer Schlüsselpaare, wobei ein Schlüssel jedes Paares nur zur Verschlüsselung dient, während der andere zur Entschlüsselung benutzt werden kann. Kann aus dem Verschlüsselungsschlüssel der Entschlüsselungsschlüssel nicht mit leistbarem Aufwand hergeleitet werden, dann spricht nichts dagegen, den Verschlüsselungsschlüssel zu veröffentlichen und nur den Entschlüsselungsschlüssel geheim zu halten. Dann ist das Wissen von Verschlüsseler und Entschlüsseler asymmetrisch: Ersterer kennt nur den veröffentlichten Verschlüsselungsschlüssel, letzterer kennt beide. Wegen der Möglichkeit der Veröffentlichung der Verschlüsslungsschlüssel heißt diese asymmetrische Kryptographie auch „Kryptographie mit öffentlichen Schlüsseln“ (Public-Key Cryptography). Da diese Kryptographie sehr umfangreiche Berechnungen erfordert, ist sie nicht von Hand durchführbar, sondern erfordert Rechnerunterstützung. Dies kann in der Form von Software geschehen – Pretty Good Privacy (PGP) ist das bekannteste Beispiel – oder in der Form von Hardware. Künftig wird Software nicht nur benutzt werden, um zwischen PCs beispielsweise E-Mail und Telefonate zu verschlüsseln. Auch bei Mobiltelefonen kann man auf teure Spezialchips zur Verschlüsselung von Telefonaten verzichten, indem man auf ihre integrierte Programmierbarkeit zurückgreift, konkret: auf eine Java-Ausführungsumgebung.

Möglichkeiten der Steganographie

Steganographie ist die uralte Kunst und die junge Wissenschaft davon, vertraulich zu haltende Nachrichten so in umfangreichere, unauffällig harmlos wirkende Hüllnachrichten hineinzucodieren, dass dies außer vom intendierten Empfänger der vertraulichen Nachricht von niemand entdeckt werden kann. Damit geht Steganographie darüber hinaus, was Verschlüsselung leisten kann, da bei Verschlüsselung immerhin noch entdeckt werden kann, dass vertraulich kommuniziert wird,

auch wenn bei beiden Techniken nicht verstanden werden kann, was der Kommunikationsinhalt ist.

Die klassische Low-Tech-Variante von Steganographie sind Codebücher,[4] die so gewählt sind, dass auch die verschlüsselte Nachricht eine unauffällig plausible Nachricht darstellt. Andere klassische Low-Tech-Varianten nehmen etwa die Summe einzelner Abschnitte der Hüllnachricht als die vertrauliche Nachricht.

In den letzten zehn Jahren wurde die Benutzung von Steganographie sehr vereinfacht und ihr Einsatzbereich deutlich gesteigert, indem für Digitalrechner geeignete steganographische Verfahren entwickelt wurden, die beliebige vertrauliche Nachrichten automatisch in digitalisierte Bilder, Tondateien, Videokonferenzen oder andere Hüllnachrichten einbetten. Während die erste Generation rechnergestützter Steganoverfahren nur für den mit seinen normalen Sinnesorganen ausgerüsteten Menschen unauffällig war, aber bei Einsatz rechnergestützter, unter anderen mathematischer, Hilfsmittel leicht enttarnt werden konnte, sind die jetzigen guten Verfahren auch mit Hilfsmitteln nicht oder nur noch schwer zu enttarnen. Zusätzlich wurde die Einbettungseffizienz deutlich gesteigert: Bei Verschlüsselung ist die verschlüsselte Nachricht nicht oder zumindest nicht wesentlich länger als die unverschlüsselte, während bei Steganographie die Hüllnachricht, in die die vertrauliche Nachricht eingebettet wird, deutlich umfangreicher ist. Früher war dies bei vorsichtig dimensionierten Verfahren üblicherweise das Hundertfache, heutzutage oftmals nur noch das Zehnfache, wodurch ganz andere Einsatzbereiche möglich werden.[5]

2.2 Begrenzung von Schutzmöglichkeiten?

Um Überwachung zu ermöglichen, wird erwogen, Anonymisierung, Verschlüsselung und Steganographie insgesamt zu verbieten oder die Verwendung bestimmter Verfahren vorzuschreiben, denen die Bedarfsträger gewachsen sind oder die von ihnen kontrolliert werden.

Solche Maßnahmen sind für Terrorismus- und Kriminalitätsbekämpfung nicht nur weitestgehend unwirksam, sondern sie fördern beides sogar:

Gesetzesbrecher werden sich nicht ausgerechnet an solch ein Verbot oder solch eine Vorschrift halten, wenn die von ihnen gewünschten Schutzmöglichkeiten zur Verfügung stehen oder sogar außerhalb des Geltungsbereichs des Verbots oder der Vorschrift weiterentwickelt bzw. angeboten werden und, da es sich entweder um kleine Geräte oder einfach nur Software handelt, problemlos importiert werden können. Manche Anonymisierungstechniken und insbesondere Kombinationen

---

4 S. Kap. 2.1.2.

5 S. z.B. www.inf.tu-dresden.de/~aw4/publikationen.html#Steganographie.

von Verschlüsselung und Steganographie können Gesetzesbrecher so einsetzen, dass ihr Einsatz nicht bemerkt und erst recht nicht verhindert werden kann.[6]

Umgekehrt wird der Schutz für Gesetzestreue reduziert, die dadurch auch von Terroristen und insbesondere Kriminellen leichter und zielgerichteter als Opfer ausgewählt, detailliert beobachtet und lokalisiert werden können. Dies gilt für Bürger wie für Firmen, es betrifft den Verlust an Privatsphäre wie die Erleichterung von Industriespionage.

Im Ergebnis gilt: Netzbezogene vorbeugende Begrenzungen von Schutzmöglichkeiten sind nicht dazu geeignet, Internetkriminalität einzudämmen. Sinnvoller ist, an der Quelle und der Senke der Kommunikation, das heißt dem Teilnehmerendgerät, anzusetzen, wo die Adressinformation und die vertrauliche Nachricht jeweils im Klartext vorliegen. Hilfsmittel hierfür reichen von der Auswertung und Aufzeichnung der elektromagnetischen Abstrahlung der Endgeräte bis hin zur Installation von Abhörtechnik in den Geräten Verdächtiger. Letzteres kann sowohl mittels kleiner Zusatzhardware wie auch geeigneter Zusatzsoftware erfolgen. Gefahrenabwehr und Strafverfolgung sollten sich also der Informationstechnik zur Individualüberwachung bedienen und nicht versuchen, sie so zu regulieren, dass sie massenüberwachungstauglich wird.

2.3 Gezielte und verhältnismäßige Überwachung

Das Maß der Ausstattung des Staats mit Machtmitteln und Eingriffskompetenzen muss die Optimierung der Freiheit aller sein. Die Machtausübung des Staats ist kein Selbstzweck, sondern hat nur dienende Funktion. Sie muss im Endeffekt zu mehr und darf nicht zu weniger Freiheit führen. Sie darf nicht die Freiheit gefährden, die sie schützen soll.

Wie aber können Freiheitssicherung und der Schutz der offenen und verletzlichen Gesellschaft gegenüber fanatisierten Terroristen gemeinsam gewährleistet werden? Nur dadurch, dass wir verhindern, dass die Normalität von der Ausnahmesituation her gestaltet wird.

Erforderlich sind rechtliche und technische Möglichkeiten, in Ausnahmesituationen höchster Bedrohung aktuell und punktuell, d.h. auf Täter und Verdächtige sowie ihre Ressourcen bezogen, schnell zu reagieren. Diese unvermeidlich weitgehenden Machtbefugnisse sollten aber jeweils auf den Ausnahmefall bezogen sein. Sie müssen zeitlich befristet sein sowie durch Gerichte, Datenschutzbeauftragte und Parlamente kontrolliert werden. Ist die Ausnahmesituation vorüber, sind die Ergebnisse zu bewerten, Betroffene zu informieren und nicht mehr erforderliche Daten zu löschen.

---

6 S. hierzu *Huhn*/*Pfitzmann*: Technische Randbedingungen jeder Kryptoregulierung, Datenschutz und Datensicherheit 1996, S. 23 ff.

Dagegen ist zu verhindern, dass in der Gesellschaft Strukturen verfestigt werden, die für immer überwachungsstaatliche Entwicklungen ermöglichen oder gar nahelegen. Über die Gesellschaft darf nicht ein Netz der Überwachung gespannt werden, in dem jeder gefangen wird, ohne dass bei der Beeinträchtigung von Grundrechten zwischen Verdächtigen und Unverdächtigen unterschieden wird. Die Fortentwicklung der Kommunikationsinfrastruktur darf daher nicht allein an dem Ziel orientiert werden, die Überwachung zu erleichtern. Vielmehr sind Probleme der Terrorismusbekämpfung im Kontext anderer staatlicher Aufgaben wie der Förderung von E-Commerce und E-Government zu sehen und in einer zivilen Informationsgesellschaften adäquaten Weise anzugehen:

Kompetenzen für Ausnahmesituationen sind beschränkt, kontrollierbar und korrigierbar. Strukturen, in die Überwachungsmöglichkeiten eingebaut sind, beeinträchtigen alle, sind missbrauchsanfällig, erheblich schwerer zu kontrollieren und nur sehr langfristig zu korrigieren.

3 Datenschutz im Internet

Bezogen auf die Nutzung der Informations- und Kommunikationstechnik in der Gesellschaft betrifft die Überwachung durch die Bedarfsträger und erst recht die Bekämpfung des Terrorismus nur einen ganz schmalen Bereich. Datenverarbeitung und Datenschutz betreffen dagegen alle Bereiche der Gesellschaft. Selbst wenn im Bereich der inneren und äußeren Sicherheit Korrekturen im Datenschutzrecht notwendig sein sollten, berührt dies in keiner Weise die Notwendigkeit des Schutzes von Arbeitnehmern gegenüber Arbeitgebern, von Versicherungsnehmern gegenüber Versicherungen, von Bankkunden gegenüber der Schufa, von Kunden gegenüber Internetanbietern oder von Bürgern gegenüber Auskunfteien und Adresshändlern. Der Datenschutz in all diesen Bereichen bedarf einer Überarbeitung, aber nicht im Sinn einer Beschränkung, sondern im Sinn einer Modernisierung.[7] Datenschutz muss einfacher und verständlicher sowie bezogen auf die Risiken neuer Formen der Datenverarbeitung adäquat und effektiv sein. Dies gilt insbesondere fürs Internet.

---

[7] Daher hat die Bundesregierung den Berliner Datenschutzbeauftragten *H. Garstka*, den Informatiker *A. Pfitzmann* und den Juristen *A. Roßnagel* beauftragt, ein Konzept und erste Vorschläge für eine solche Modernisierung zu erarbeiten, s. *Roßnagel/Pfitzmann/Garstka,* Modernisierung des Datenschutzrechts, Gutachten für das Bundesinnenministerium, Berlin 2001, abrufbar unter www.bmi.bund.de, www.datenschutz.de oder www.emr-sb.de.

3.1 Risiken des Internet

Die Nutzung des Internet hat dazu geführt, dass nahezu alle sozialen Handlungen auch auf dieses Medium übertragen werden. Die Abwicklung wirtschaftlicher, gesellschaftlicher, politischer und persönlicher Beziehungen über das Internet wird künftig in starkem Ausmaß zunehmen. Im Gegensatz zur Offline-Welt wird in der Online-Welt aber jede Lebensregung Datenspuren erzeugen, die in unmittelbar verarbeitbarer Form entstehen. Diese personenbezogenen Daten haben einen steigenden Wert und eine wachsende Bedeutung für die Informationswirtschaft. Daher werden sie in vielfacher Weise gesammelt und zu unterschiedlichsten Profilen aggregiert, die zum Beispiel Auskunft über Interessen, Präferenzen, Kaufkraft, Kaufgewohnheiten und Kreditwürdigkeit einer Person geben. Unternehmen für Online-Werbung und Profilhändler haben aus dem Internet Millionen von Profilen mit jeweils hunderten von Merkmalen gewonnen und verkaufen diese an jeden, der zahlt. Auf deren Grundlagen wird vielfach über Dienstleistungen, Konditionen und Preise entschieden.

Tatsächlicher oder befürchteter Missbrauch von personenbezogenen Daten ist ein entscheidendes Hemmnis für die Entwicklung von E-Commerce und E-Government, Datenschutz umgekehrt ein entscheidender Akzeptanzfaktor. Er kann das notwendige Vertrauen in die elektronische Kommunikation schaffen und verbreiteten Befürchtungen entgegenwirken. Ein moderner und den neuen Technikanwendungen adäquater Datenschutz ist daher ein bedeutender Wettbewerbsfaktor und Standortvorteil, der es ermöglicht, in der Informationsgesellschaft personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen.

3.2 Modernisierung des Datenschutzes

Um das Ziel einfacher und verständlicher Datenschutzregeln zu erreichen, müssen die Selbstbestimmung der betroffenen Person gestärkt und die Selbstregulierung und Selbstkontrolle der Datenverarbeiter ermöglicht und verbessert werden. Um das zweite Ziel risikoadäquater Datenschutzregeln zu erreichen, muss vor allem die Transparenz der Datenverarbeitung verbessert und müssen Konzepte des Selbstdatenschutzes und des Systemdatenschutzes umgesetzt sowie die Regeln des Marktes auch für den Datenschutz genutzt werden.

Stärkung von Selbstbestimmung und Selbstregulierung

Eine spürbare Entlastung des Datenschutzrechts wird nur möglich sein, wenn der Gesetzgeber nicht mehr für alle Fälle die Konfliktlösungen selbst festlegt, sondern sie vielfach der autonomen Konfliktlösung der Parteien überlässt. Hierzu muss die Privatautonomie auch im Datenschutzrecht konsequent berücksichtigt und die Einwilligung zum vorrangigen Legitimationsgrund der Datenverarbeitung werden. Die Erlaubnistatbestände zur zwangsweisen Datenverarbeitung sind daher über-

wiegend durch das „Opt-in-Prinzip“ zu ersetzen. Da aber zwischen den Parteien in der Regel ein erhebliches Machtgefälle besteht, muss das Datenschutzrecht die Freiwilligkeit der Einwilligung sichern. Daneben ist eine Selbstregulierung der Datenverarbeiter zu ermöglichen, freilich innerhalb eines rechtlichen Rahmens, der die Zielerreichung sicherstellt und bei einem Versagen der Selbstregulierung Ersatzmaßnahmen vorsieht.

Stärkung der Transparenz

Informationelle Selbstbestimmung erfordert Transparenz. Damit die betroffene Person wissen kann, „wer was wann und bei welcher Gelegenheit über sie weiß“,[8] muss sie die Möglichkeit haben, die Bedingungen der Datenverarbeitung zur Kenntnis zu nehmen, bevor von ihr personenbezogene Daten erhoben werden. Hier bietet der weltweite Datenschutzstandard des W3C „Platform for Privacy Preferences (P3P)“[9] die technische Unterstützung für die Grundregel des „Notice and Choice“ (Benachrichtigung und Wahlmöglichkeit). Publiziert die verantwortliche Stelle eine Datenschutzerklärung im WWW, die dem P3P-Standard entspricht, kann der Nutzer seine Datenschutzpräferenzen automatisiert mit der Datenverarbeitungspraxis der verantwortlichen Stelle abgleichen. Seine P3P-Software gibt ihm „grünes Licht“ oder warnt ihn vor unzumutbaren Bedingungen. Er kann dann entscheiden, ob er die Bedingungen akzeptiert oder die Verbindung zu der verantwortlichen Stelle abbricht.

Systemdatenschutz

Fallen irgendwo im Internet personenbezogene Daten an, kann die betroffene Person sie nicht mehr wirksam kontrollieren oder gar ihre Löschung durchsetzen. Informationelle Selbstbestimmung ist nur dadurch möglich, dass die betroffene Person darüber entscheiden kann, ob von ihr überhaupt personenbezogene Daten entstehen. Entscheidend sind daher Möglichkeiten zur Vermeidung der Entstehung von Daten oder ihres Personenbezugs.

In einer technischen Umgebung wie dem Internet hat Datenschutz nur eine Chance, wenn er in Technik integriert ist. Dieser Ansatz bietet zwei Vorteile. Im Gegensatz zu nationalem Datenschutzrecht ist Datenschutztechnik weltweit wirksam und Technikunternehmen sind – im Gegensatz zu Gesetzgebern – sehr schnell lernende Systeme, die auf jede technische Gefährdung meist ebenso schnell technische Antworten finden.

Techniken zum Datenschutz sind zu ergänzen durch Regelungen zum Systemdatenschutz. Diese sollen sicherstellen, dass technisch-organisatorische Systeme nur zu der Datenverarbeitung in der Lage sind, zu der sie rechtlich auch ermächtigt

---

8 Entscheidungen des Bundesverfassungsgerichts, Bd. 65, S. 43.

9 S. www.w3c.org/P3P/.

sind. Die technisch-organisatorischen Verfahren sind so zu gestalten, dass – so weit möglich – auf die Verarbeitung von Daten verzichtet wird oder die zu verarbeitenden Daten keinen Personenbezug aufweisen. Letzteres ist möglich, indem von Anfang an anonymes oder pseudonymes Handeln ermöglicht wird oder personenbezogene Daten frühestmöglich anonymisiert oder pseudonymisiert werden. Vorsorgeregelungen müssen sicherstellen, dass keine unbeabsichtigte Aufdeckung der anonymen oder pseudonymen Daten möglich ist und das Schadenspotenzial einer Aufdeckung reduziert wird.

Selbstdatenschutz

Da Staat und Recht im globalen Internet nur begrenzt in der Lage sind, die informationelle Selbstbestimmung ihrer Bürger zu schützen, sollte dem Bürger ermöglicht werden, Mittel zu ergreifen, um seine informationelle Selbstbestimmung selbst zu schützen. Mittel hierzu wurden bereits vorgestellt. Sie werden breit angeboten und sollten nicht nur denjenigen vorbehalten werden, die sich außerhalb des Gesetzes stellen.[10]

Marktwirtschaftliche Anreize für Datenschutz

Datenschutz kann nicht allein auf rechtliche Ge- und Verbote setzen und sich auf nachträgliche Kontrollen verlassen. Er muss vielmehr auch die Mechanismen des Wettbewerbs nutzen, um Anreize zu schaffen, System- und Selbstdatenschutz umzusetzen. Anforderungen zur Optimierung des Datenschutzes und der Datensicherheit werden nur dann umzusetzen sein, wenn hierfür Eigeninteressen und Eigeninitiative mobilisiert werden.

Dies kann etwa erreicht werden, indem in einem freiwilligen Datenschutzaudit bestätigt wird, dass das Datenschutzmanagementsystem geeignet ist, eine kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit zu erreichen, und daraufhin die verantwortliche Stelle im Wettbewerb ein Auditzeichen führen darf.[11] Auch sind vertrauenswürdige Zertifizierungen datenschutzgerechter und –förderlicher Produkte notwendig, die durch die rechtliche Anforderung begleitet werden, diese bei Beschaffungen der öffentlichen Hand zu bevorzugen. Schließlich wäre an Erleichterungen hinsichtlich rechtlicher Anforderungen zu denken, wenn eine hohe Transparenz der Datenverarbeitung sichergestellt wird, wenn Audits erfolgreich bestanden wurden oder wenn zertifizierte datenschutzfreundliche Produkte verwendet werden.

---

10 S. Kap. 2.1.

11 S. hierzu näher *Roßnagel*, Datenschutzaudit – Konzeption, Durchführung, Gesetzliche Regelung, Braunschweig 2000.

4 Ausblick

Die Novellierung des Datenschutzrechts und die hier vorgestellten Vorschläge sind durch die Terroranschläge vom 11. September 2001 und die anschließenden Ausweitungen der Kompetenzen der Bedarfsträger nicht obsolet geworden. Im Gegenteil sind sie als Ausgleich für die in diesem Zusammenhang erfolgten Einschränkungen des Datenschutzes wichtiger denn je. Sofern nicht zur Terrorismusprävention ein grundgesetzwidriges Netz einer potenziell allgegenwärtigen und umfassenden Überwachung aller Aktivitäten – insbesondere in der Telekommunikation – gespannt werden soll, sind die Vorschläge auch mit den berechtigten Interessen der Bedarfsträger vereinbar: Intensivere Überwachung in Ausnahmebereichen, gestärkter Datenschutz im Normalfall.[12]

[12] S. hierzu auch *Roßnagel*, Freiheit im Cyberspace, Informatik-Spektrum 1/2002, S. 33 ff.