in: Kubicek et. al. (Hrsg.): „ Internet @ Future “, Jahrbuch Telekommunikation und Gesellschaft 2001, Hüthig Verlag, 2001, 252-259

Neues Datenschutzrecht und die Technik

Hannes Federrath • Freie Universität Berlin • Institut für Informatik
Andreas Pfitzmann • TU Dresden • Fakultät Informatik

Ausgangssituation für den Datenschutz heute

Ein Ziel der Novellierung des BDSG ist die Anpassung der Regelungen an die neuen Gegebenheiten der Informationsgesellschaft. Die Bedingungen für die Durchsetzung von Datenschutz bei der Datenverarbeitung haben sich in den vergangenen zwanzig Jahren teilweise grundsätzlich geändert.

Daten werden heute größtenteils dezentral erhoben, gespeichert und verarbeitet. Kopien riesiger Datenmengen können verlustfrei und ohne nennenswerte Kosten in Sekundenschnelle über den gesamten Erdball gesendet werden.

Die Speicher und Datenverarbeitungsgeräte (inkl. ihrer inzwischen multimedialen Eingabegeräte) sind dermaßen klein und kostengünstig geworden, dass nahezu an jedem Ort auch unbemerkt Daten erfasst und verarbeitet werden können.

Private bzw. nicht öffentliche Stellen speichern und verarbeiten inzwischen mit hoher Selbstverständlichkeit personenbezogene Daten, deren Sensitivität gegenüber den bei öffentlichen Stellen gespeicherten nicht geringer ist.

Die Informations- und Kommunikationsangebote des Internet befriedigen heute nahezu jedes Bedürfnis nach Wissen, Unterhaltung und Informationsaustausch. Bei jeder Interaktion hinterlässt der Teilnehmer dabei vielfältige Datenspuren, sowohl beim Kommunikationspartner als auch bei dazwischen liegenden Routern. Kommunikationsverbindungen sind weitgehend ungeschützt gegen Verfälschung und Mitlesen.

Die Verlässlichkeit, Erreichbarkeit und Verfügbarkeit von Diensten und Kommunikationspartnern kann größtenteils nicht garantiert werden. Eine Gesellschaft, die sich vom Funktionieren der Informationstechnik stark abhängig macht, wird verletzbar durch Denial-of-Service-Angriffe, unvorhergesehene Netzausfälle und Überlastungssituationen.

Der Betroffene kann und darf sich nicht mehr allein darauf verlassen, dass der Staat oder die speichernde und verarbeitende Stelle genügend unternehmen werden, um den Betroffenen zu schützen. Während früher wenige Großrechner und Datenbanken durch wenige Betreiber, die vergleichsweise leicht kontrolliert werden konnten, bedient wurden, sind heute alle Betroffenen selbst Betreiber und Teilnehmer an der Datenverarbeitung. Diese neue Situation führt dazu, dass sich der Teilnehmer auch selbst um seine eigene und die Sicherheit anderer kümmern muss.

Neue Datenschutzrisiken

Die Großrechner vor 20 Jahren waren streng bewacht: Für sie galten Zugangskontrollmaßnahmen (Pförtner, Stahltüren etc.), die nicht leicht zu überwinden waren. Die Vernetzung von Rechnern blieb Spezialanwendungen vorbehalten. Da personenbezogene Daten meist auf diesen zentralisierten Datenverarbeitungssystemen gespeichert wurden, waren die Daten, verglichen mit der Speicherung in den heutigen über das Internet verbundenen Systemen, gut gesichert: Mit dem Einzug des Internet und der Mobilkommunikation in alle Bereiche des Lebens fallen personenbezogene Daten in einer noch nie dagewesenen Menge an, deren Schutz selbst von den Betroffenen teilweise erstaunlich locker gesehen wird. Für die Aussicht auf ein kostenloses „Goodie“ werden Namen, Adressen und Telefonnummern im Internet preisgegeben; Kreditkartennummern werden über das unsichere Internet übertragen, um Waren und Dienstleistungen zu bezahlen. Globally Unique Identifier, Prozessor IDs und Ethernetadressen können einen Menschen, der einen Großteil seiner Aktivitäten „ins Netz“ verlagert, fast vollständig beobachtbar machen, da sie als Personenkennzeichen fungieren. Bereits vor 10 Jahren genügte die Speicherkapazität eines tragbaren Mediums (Magnetbandkassette), um die personenbezogenen Daten der Volkszählung von 1987 (knapp 2 Gigabyte) der Bürger der Bundesrepublik aufzunehmen. Auf vergleichbaren, heute verfügbaren Speichermedien fänden zusätzlich noch hoch auflösende Fotos aller Bürger mitsamt den Fotos Ihrer Wohnhäuser Platz. Durch die Vernetzung ist es möglich, solche Datenmengen blitzschnell an das andere Ende der Welt zu transportieren. Private Haushalte können heute mit Übertragungskapazitäten zwischen 500 Kilobit/s und 1 Megabit/s angeschlossen werden. In ein paar Jahren wird sich die Übertragungskapazität von und zu privaten Haushalten verhundertfacht haben. Die verfügbaren Speichermedien, Netze und Übertragungsgeschwindigkeiten ermöglichen die kostengünstige und schnelle Vervielfältigung und Verbreitung auch von personenbezogenen Daten. Sie sind für den Betroffenen und seine Kommunikationspartner (und ggf.

auch Unberechtigte) stets verfügbar, kaum endgültig löschbar, weil vielfach dupliziert, die Integritätssicherung erfordert viel Mühe bzw. ist nicht mehr möglich. Glücklicherweise existieren einerseits Datenschutzgesetze, andererseits Technik, die die Menschen schützen können. Technik kann dabei Daten und Menschen schützen: Während *Datensicherheit* die Daten schützen soll, schützt *Datenschutz* die Menschen. Datenschutz betrifft den Gebrauch von personenbezogenen Daten durch Berechtigte. Datensicherheit betrifft den Schutz von Daten vor Missbrauch, Fälschung und Verlust bzw. Nicht-Verfügbarkeit. Datenschutz ist primär aus der Sicht des Betroffenen interessant, während Datensicherheit primär die Sicht des Datenverarbeiters und -besitzers betrachtet.

Datenschutz durch Technik

Eine Qualität des neuen Datenschutzes ist die stärkere Berücksichtigung der technischen Möglichkeiten für die Verbesserung des Datenschutzes bei der Neufassung von Datenschutzregelungen. Datenschutz durch Technik bedeutet, dass sich die Gestaltung von Technik im Hinblick auf die Verarbeitung personenbezogener Daten am Ziel Datenschutz orientiert. Dabei kann Technik einerseits die *Vertraulichkeit* von personenbezogenen Daten schützen, aber auch deren *Korrektheit* (inkl. ihrer Aktualität).
Wann immer möglich, sollten personenbezogene Daten vollständig vermieden werden (Datenvermeidung) oder wenigstens so wenig wie möglich personenbezogene Daten verarbeitet werden (Datensparsamkeit).
Datenvermeidung: Die Vertraulichkeit von Daten ist dann am größten, wenn sie vollständig vermieden werden können – was natürlich nur bei für eine bestimmte Zweckerfüllung nicht benötigten Daten möglich ist. Dabei ist erstaunlich, wie viele einen Personenbezug herstellende Daten sich als unnötig herausstellen, wenn nur früh und gründlich genug nachgedacht und das System entsprechend gestaltet wird. Beispielsweise ist es keineswegs erforderlich, dass der einen Telekommunikationsdienst Erbringende erfährt, welche Kommunikationspartner er miteinander verbindet.
Datensparsamkeit: Kann man personenbezogene Daten nicht vermeiden, so ist das Nächstbeste, die Verwendungsmöglichkeit notwendiger Daten einzuschränken bzw. Betroffenen die Möglichkeit zu geben, die Daten insbesondere bei jeder Verwendung auf Richtigkeit und Aktualität zu überprüfen. Das Ziel der Datensparsamkeit umfasst, die Verwendungsmöglichkeit notwendiger Daten einzuschränken.

Datensicherheit als Grundschutz

Zweifellos vereinfacht die existierende Informationstechnik nahezu alle Geschäftsprozesse, in denen Daten verarbeitet und gespeichert werden müssen. Diesen positiven Folgen stehen erhöhter Aufwand für die Datensicherheit und den Datenschutz gegenüber. Maßnahmen wie ein Sicherheitsmanagement, Backup, Zugangs- und Zugriffskontrolle zählen dabei zu den Grundschutzmaßnahmen, die unternommen werden, um einerseits den gesetzlichen Anforderungen gerecht zu werden, und andererseits, um sich nicht selbst seiner Geschäftsgrundlage, den gespeicherten Daten, zu berauben oder sie in die Hände des Wettbewerbers zu spielen.

Naturgemäß investieren Unternehmen vorrangig für die *Datensicherheit*, um sich vor empfindlichen Angriffen durch Industriespionage und Hacker zu schützen, was nebenbei auch der Verbesserung des *Datenschutzes* zugute kommt.

Mehrseitige Sicherheit durch Technik

Wenn Technik zur Datenverarbeitung und -speicherung eingesetzt wird, erscheint es eigentlich selbstverständlich, Technik auch zum aktiven Datenschutz und zur Datenvermeidung einzusetzen.
Es ist völlig unklar und unverständlich, warum die rechtmäßige Datenverarbeitung mit Hilfe von Technik gerne genutzt wird, um Kosten zu sparen und effizient handeln zu können, gleichzeitig aber der Aufwand gescheut wird, Technik einzusetzen, mit der Geschäftsprozesse so abgewickelt werden, dass personenbezogene Daten vollständig vermieden oder wenigstens stark reduziert werden. Gesteigerte Effizienz eines Unternehmens durch elektronische Datenverarbeitung darf kein Argument für reduzierten Datenschutz zu Lasten des Betroffenen sein. Zwar kann mit jeder Datenverarbeitung die Einwilligung des Betroffenen eingeholt werden, um auf niedrigem Datenschutzniveau trotzdem verarbeiten zu dürfen; im Endeffekt unterhöhlt aber dieses Vorgehen die Rechte des Betroffenen, weil sie „daran gewöhnt“ werden, dass es ohne die Preisgabe ihrer persönlichen Daten angeblich nicht möglich ist, bestimmte Dienstleistungen in der Informationsgesellschaft in Anspruch zu nehmen.
Die Vertrauensverhältnisse zwischen den verschiedenen beteiligten Instanzen innerhalb eines IT-Systems entscheiden stark darüber, welches Schutzniveau für den einzelnen Beteiligten tatsächlich erreicht werden kann. Nicht selten gilt dabei, wie im wirklichen Leben, dass die Mächtigen ihre Interessen gegen die schwächeren Partner durchsetzen, zumindest solange sie dies auf legaler Basis tun können. Man könnte diesen Prozess mit dem evolutionären Grundgedanken, dass der (genetisch) Stärkere den Überlebenskampf gewinnt, erklären und billigen. Glücklicherweise hat sich in den letzten Jahren eine Gegenströmung im Bereich der IT-Sicherheit etabliert, die dieser einseitigen Betrachtung von Sicherheit und Schutz das Konzept der mehrseitigen Sicherheit entgegenstellt.
Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung. Die Realisierung von mehrseitiger Sicherheit führt nicht zwangsläufig dazu, dass die Interessen aller Beteiligten erfüllt werden. Sie gewährleistet jedoch, dass die Partner einer mehrseitig sicheren Kommunikation in einem geklärten Kräfteverhältnis bzgl. Sicherheit miteinander interagieren.
Die mehrseitige Sicherheit verbindet die Sichtweisen von Datenschutz und Datensicherheit zu einem gemeinsamen Konzept. Während sich Datenschutz hauptsächlich um die Interessen der Betroffenen kümmert, und Datensicherheit vor allem die Interessen der Datenbesitzer und -verarbeiter beachtet, wird bei mehrseitiger Sicherheit in einem Aushand-

lungsprozess versucht, möglichst Beides, Datenschutz und Datensicherheit zu gewährleisten. Dies trägt der Entwicklung Rechnung, dass aus den bisher lediglich Betroffenen zunehmend informationstechnisch Beteiligte werden können und oftmals werden sollten.

Sicherung der Vertraulichkeit

Vertraulichkeit lässt sich unterteilen nach der Vertraulichkeit der Kommunikationsinhalte und der Vertraulichkeit von Kommunikationsumständen. Das Zweite kann in der Praxis etwas enger als Anonymität und Unbeobachtbarkeit aufgefasst werden und wird später in einem eigenen Abschnitt behandelt.
Kommunikationsinhalte lassen sich heute sehr effizient und sicher gegenüber allen potenziellen Lauschern einer Kommunikation schützen, indem sie verschlüsselt werden. Gute Verschlüsselungsverfahren (z.B. Triple-DES, IDEA, Advanced Encryption Standard) sind heute so gut untersucht und so weit verbreitet, dass sie kaum realistische Angriffspunkte für eine verborgene Verletzung der Vertraulichkeit bieten. Nahezu alle bekannten Schwächen existierender Krypto-Software beruhen nicht etwa auf Fehlern in den mathematischen Zusammenhängen, sondern sind entweder auf unzulängliche, fehlerhafte Implementierungen zurückzuführen oder auf erfolgreiche Angriffe auf den Rechner oder das Betriebssystem, auf dem die Software eingesetzt wurde.

Zurechenbarkeit und Pseudonymität

Die technische Funktion zur Realisierung von Zurechenbarkeit ist die Digitale Signatur. Digitale Signaturen realisieren die Echtheit eines digitalen Dokumentes. Jeder, der Unterzeichner, der Empfänger und jeder Dritte kann die Echtheit eines Dokuments, d.h. die Zusammengehörigkeit der Digitalen Signatur zum Dokument und Schlüssel überprüfen. Die Zurechenbarkeit kommt dadurch zustande, dass dem Unterzeichner ein Schlüsselpaar eindeutig zugeordnet ist, dessen Echtheit bzw. Zugehörigkeit zu der betreffenden Person ebenfalls durch die Digitale Signatur einer Zertifizierungsstelle bestätigt wurde.
Digitale Signaturen sind aus Datenschutzsicht besonders deshalb nützlich, weil sie bei Existenz von Fehl- oder Falschinformation auch deren Urheber authentisieren. Das ermöglicht dem Betroffenen ein gezieltes Vorgehen zur Korrektur und Löschung.
Umgekehrt ist es nicht gerade im Interesse eines Betroffenen, wenn jedes von ihm ausgelöste Kommunikationsereignis stets zurechenbar sein muss, beispielsweise durch das erzwungene Leisten einer digitalen Signatur unter jeder versendeten E-Mail. Nur noch authentisierte Informationen abgeben zu können, führt auf Dauer zu einem Verlust an informationeller Selbstbestimmung und auch an Datenschutz, wenn beispielsweise jeder Besuch einer Webseite damit verbunden wäre, sich zu authentisieren und den Abruf der Seite digital zu signieren.
Glücklicherweise existiert aber auch die technische Möglichkeit, digitale Signaturen unter Pseudonym zu leisten. Ein Betroffener generiert sich in diesem Fall beliebig viele Pseudonyme und lässt sie sich von einer Zertifizierungsstelle bestätigen, d.h. die Zertifizierungsstelle bestätigt, dass sie die Identität des Pseudonyminhabers kennt und im Streitfall aufdecken kann. Zu jedem Pseudonym gehört auch ein Schlüsselpaar für Digitale Signaturen, mit dem schließlich Transaktionen zurechenbar, aber trotzdem pseudonym erfolgen können. Solche Techniken sind momentan noch nicht ausreichend verfügbar, es ist aber lediglich eine Frage der Zeit, wann entsprechende Anbieter auf den Markt drängen. Derartige Pseudonymkonzepte werden neuerdings auch unter dem Begriff *Identitätsmanagement* gehandelt.
Bei Transaktionen mit entsprechend niedrigem Streitwert kann das geschilderte Verfahren folgendermaßen abgewandelt werden: Die Zertifizierungsstelle erhält vom Pseudonyminhaber anstelle der Identität einen Geldbetrag zur Hinterlegung. Im Streitfall kann die Zertifizierungsstelle zwar nicht die Identität des Betroffenen aufdecken, wohl aber bis zur Höhe des hinterlegten Geldbetrages den Schaden regulieren.

Verteilung von Kontrolle

Um Vertrauenswürdigkeit von Technik zu erreichen, muss es möglich sein, Systeme zu validieren. Das bedeutet, unabhängige, (frei) wählbare Experten vergewissern sich von der korrekten Implementierung und Arbeitsweise eines Systems gemäß einer allgemein akzeptierten Spezifikation. Da dem normalen Anwender meist weder die Mittel noch das Wissen zur Verfügung stehen, um Systemkomponenten oder gar ganze Systeme zu validieren (geschweige denn zu verifizieren), sollte diese Aufgabe durch *unabhängige Stellen* durchgeführt und das System so zertifiziert werden.
Im weiteren Sinn bedeutet Verteilung von Kontrolle auch, dass Systeme nicht nur von *einem* Hersteller (Entwickler, Administrator) entwickelt, produziert, angeboten und betreut werden, sondern von vielen. Solange beispielsweise kein perfektes Betriebssystem existiert, sollte der Anwender die Auswahl unter mehreren Betriebssystemen haben.
Ein interessantes Konzept zur Verteilung von Kontrolle ist die Politik der Offenheit, insbesondere bei der Erstellung und Validierung von Software. *Open Source* kann helfen, „Fehler“ in Software schneller zu finden und die Qualität der Software durch Verfügbarkeit von allgemein nutzbaren Modulen zu verbessern. Im Sicherheitsbereich ist Offenheit ohnehin ein gutes Mittel zur Erhöhung der Vertrauenswürdigkeit. Kein Kundiger würde der Sicherheit eines Verschlüsselungsalgorithmus ernsthaft vertrauen, wenn dieser nicht öffentlich bekannt und durch Experten auf Sicherheitslücken geprüft worden ist.

Anonymität und Unbeobachtbarkeit

Für einen Benutzer des Internet sollte es wie im „wirklichen Leben“ die Möglichkeit geben, wann immer er es wünscht, seine Identität vor Anderen zu verbergen, d.h. seine Anonymität zu wahren. Wer einen Laden betritt, um sich nur zu informieren, stellt sich dem Verkaufspersonal auch nicht mit vollem Namen und Adresse vor, sondern bleibt zunächst anonym. Ein Besuch eines Internet-Shops beginnt heutzutage meist mit dem Übermitteln eines Cookies. Auf jeden Fall

aber hinterlässt der Besucher bereits mit dem ersten Klick seine Internet-Adresse.
Bei *anonymer* Kommunikation verbirgt ein Kommunikationspartner seine Identität vor den anderen Kommunikationspartnern. Bei *unbeobachtbarer* Kommunikation kennen sich möglicherweise die Kommunikationspartner, allerdings kann niemand sonst, nicht einmal die Betreiber des Kommunikationsnetzes, feststellen, dass die Kommunikationspartner miteinander kommunizieren.
Auch für Unbeobachtbarkeit findet man Anwendungen im wirklichen Leben: Firmen möchten möglichst unbeobachtbar Patentrecherchen betreiben, um eigene Forschungen und Entwicklungen vor der Konkurrenz geheim zu halten. Beratungsstellen sollten kontaktiert werden können, ohne dabei Datenspuren beim Netzbetreiber zu hinterlassen.
Durch Anonymität ist geschützt, wessen Handlungen innerhalb einer sog. Anonymitätsgruppe nicht mit seiner Identität verkettbar sind. Da typischerweise eine Handlung nur dann anonym ist, wenn sie durch einen Angreifer nicht ihrem Urheber zugeordnet werden kann, müssen mehrere unterschiedliche und nicht angreifende Parteien innerhalb einer Anonymitätsgruppe agieren. Deshalb ist Anonymität nur multilateral, d.h. unter Mithilfe Vieler erreichbar. Die Handlung einer isoliert agierenden einzelnen Person kann nie anonym erfolgen.
Mittels spezieller Schutzmechanismen kann jedoch die Anonymität und Unbeobachtbarkeit des Nachrichtenaustauschs allgemein und speziell des Sendens und Empfangens von Nachrichten erreicht werden. Die hierzu verwendeten Mechanismen nutzen meist kryptographische Basismechanismen in speziellen Kommunikationsprotokollen und/oder speziellen Nachrichtenformaten aus.

Es ist nicht das primäre Interesse eines Betreibers, beispielsweise Daten über seine Nutzer zu sammeln, um diese anschließend missbräuchlich zu verwenden. Im Gegenteil: Je weniger Daten ein Betreiber zur Diensterbringung benötigt, umso weniger Kosten fallen für deren Verarbeitung und Schutz an. Außerdem reduzieren sich die Missbrauchsmöglichkeiten. Insofern führen Datenvermeidungstechniken langfristig nicht nur zu einer Verbesserung des *Datenschutzes*, sondern reduzieren gleichzeitig den Aufwand für die *Datensicherheit*.

Bekannte Schutzmechanismen für Anonymität und Unbeobachtbarkeit sind der Schutz des Empfängers durch Verteilung (Broadcast), wie z.B. der heute noch übliche Rundfunk- und Fernsehempfang über Antenne oder Breitbandverteilkabel, Mixe zum Schutz der Kommunikationsbeziehung von Sender und Empfänger, die zunehmend im Internet angewendet werden, z.B. bei anonymen Remailern (Mixmaster), beim Anonymen Surfen (Freedom, Java Anon Proxy, Onion-Routing).
Diese Techniken sind verfügbar und teilweise schon recht effizient nutzbar. Allerdings erfordern sie stets eine aktive und bewusste Entscheidung für den Einsatz, da solche Software bisher nicht zum Leistungsumfang von Betriebssystemen, E-Mail-Programmen und Browsern gehört. Die massenhafte Nutzung und damit der Grundschutz wird erst eintreten, wenn diese Software zum Standardumfang von Softwarepaketen gehört.

Sicherung der Zweckbindung

Aus Datenschutzsicht ist es wünschenswert, wenn auch komplexere rechtliche Ziele durch Technik unterstützt werden. Durch Datenvermeidungs- und Datensparsamkeitstechniken wird beispielsweise die unberechtigte Kenntnisnahme und Veränderung personenbezogener Daten verhindert, d.h. die Vertraulichkeit und Integrität von Daten kann durch kryptographische Mechanismen geschützt werden. Die Anonymität und Unbeobachtbarkeit von Menschen kann durch datenschutzfreundliche Kommunikationsnetze (Breitbandverteilung, Mixe) erreicht werden. Die *technische Sicherung der Zweckbindung* gestaltet sich schwieriger. Leider gibt es kaum technischen Hilfen, die Zweckbindung sicherstellen, etwa das Verhindern der unberechtigten Übermittlung von Daten, die man berechtigterweise zur Kenntnis bekommen hat.
Daten können z.B. Kennzeichen (*tags*) des Zwecks ihrer Erhebung mitgegeben werden, d.h. personenbezogene Daten werden mit ihrem Zweck gespeichert. Auf beides kann nur von ausgewählten Teilen der Anwendungssoftware unter strikter Kontrolle des Betriebssystems zugegriffen werden (sog. *tagged architecture*). Dies muss so erfolgen, dass die Kennzeichen nicht wiederum missbraucht werden können, etwa zur Profilbildung.
Eine *tagged architecture* auf der Basis eines unsicheren Betriebssystems hilft natürlich nicht gegen einen Angreifer, der ernsthaft versucht, gegen die Zweckbindung zu verstoßen.
Grundsätzlich gilt: Je weniger personenbezogen die zu verarbeitenden Daten sind, umso unproblematischer ist die Zweckbindung. Feingranulare Pseudonymität kann hier helfen: Pseudonyme sind Personen nicht über mehrere Zwecke oder gar mehrere Lebensbereiche zugeordnet, sondern für jeden Zweck wird ein anderes Pseudonym verwendet.

Fazit

Vertraulichkeit und – wo vom Dienst gefordert – Zurechenbarkeit (durch Digitale Signaturen) werden zukünftig den technischen Grundschutz aus Datenschutzsicht bilden. Diese Techniken sind heute weitgehend verfügbar und ausgereift. Sie bilden das Rückgrat des Datenschutzes in IT-Systemen.
Verfahren zur unbeobachtbaren und anonymen Kommunikation, sowie Identitätsmanagement und Pseudonymität bilden zusammen mit dem technischen Grundschutz die Basis für eine mehrseitige Sicherheit, die die Interessen der Betroffenen und Verarbeiter von Daten berücksichtigt. Diese Techniken erleben derzeit ihren Übergang von der akademischen zur kommerziellen Bedeutung. Ihr Einsatz wird zukünftig ein entscheidendes Marketinginstrument sein.
Die technischen Möglichkeiten zum Schutz personenbezogener Daten haben sich in den letzten Jahren erheblich verbessert. Allerdings hat die Verarbeitung von personenbezogenen Daten ebenfalls stark zugenommen.

Naturgemäß hinkt die Entwicklung und Bereitstellung von Schutzmechanismen immer etwas der technischen Entwicklung von neuen, schnelleren Nutzfunktionen (mehr Bandbreite, schnellere Kommunikation, mehr Farbe etc.) hinterher. Dies gilt leider auch für den Datenschutz. Einmal preisgegebene, d.h. im Netz verbreitete personenbezogene Daten lassen sich wie manch andere Schäden nicht einfach wieder beseitigen. Insofern trifft die Analogie zu, dass das Internet heute etwa so sicher ist wie das Auto in den 60er Jahren ohne Sicherheitsgurte, ABS und Airbag. Es gibt eigentlich keinen Grund, die heute schon bekannten Schutzmöglichkeiten erst nach und nach einzuführen, wenn bereits heute klar ist, dass der Verzicht auf sie mit hohem Risiko verbunden ist. Dies gilt erst recht, weil die Schäden im Bereich Datenschutz schleichend sind und erst lange Zeit später bemerkt werden könnten, wenn z.B. unerwartet Datenprofile über jeden Internet-Nutzer entstanden sind. Deshalb schaden rechtliche Vorgaben für einen Datenschutz *durch* Technik weder der Wirtschaft, noch dem Menschen, noch behindern sie den technischen Fortschritt.

Anmerkung zum Schluß

Die technischen Details der genannten Verfahren wurden bewusst weggelassen, um einen Gesamtüberblick zu schaffen. Der an den konkreten Verfahren interessierte Leser findet im Internet unter www.inf.tu-dresden.de/~hf2/security/ technische Informationen und Beschreibungen der Verfahren.