Neue Konzepte für den Datenschutz – Das Internet als Herausforderung

Alexander ROßNAGEL*

1. Altes Ziel - neue Wege

Spätestens durch die breite Nutzung des Internet wird deutlich, daß der Datenschutz vor neuen Herausforderungen steht. Zum einen nehmen mit den Internet die Möglichkeiten drastisch zu personenbezogene Daten von vielen Bürgern über alltägliches Verhalten, Einstellungen und Präferenzen zu sammeln. Zum anderen werden durch das Internet Informationen und Datenverarbeitungsmöglichkeiten für jeden weltweit verfügbar. In Sekundenschnelle können ganze Datensammlungen über den Globus transferiert oder abgerufen werden. Im Internet gibt es keine Grenzkontrollen. Die Datenverarbeitung findet nicht in einer Datenverarbeitungsanlage statt, sondern im Netz mit einer Vielzahl von Beteiligten. Wer wo welche personenbezogenen Daten verarbeitet oder verarbeiten lässt, ist von einem Nationalstaat nicht mehr zu kontrollieren. Zwar findet das Datenschutzrecht der Bundesrepublik Deutschland immer dann Anwendung, wenn der Datenverarbeiter seinen Sitz in Deutschland hat.[1] Gegenüber Datenverarbeitern, die über das Internet vom Ausland aus agieren, ist das deutsche Datenschutzrecht jedoch machtlos.[2]

Die neue Herausforderungen lassen das bisherige Datenschutzrecht überholt erscheinen. Das Grundgesetz, die Verfassung der Bundesrepublik Deutschland, verbürgt zwar hat jedem Bürger ein Grundrecht auf informationelle Selbstbestimmung.[3] Grundsätzlich soll er darüber entscheiden können, ob und welche Daten über ihn von anderen gesammelt und verwendet werden. Dieses Selbstbestimmungsrecht kann aber vom

---

* Prof. Dr. Roßnagel ist Universitätsprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel. Der Beitrag entstand im Forschungsprojekt „Datenschutz in Telediensten (DASIT)“, das von der DG-Bank, Frankfurt, der GMD-Forschungszentrum Informationstechnik, Darmstadt, und Universität Kassel, Projektgruppe verfassungsvertragliche Technikgestaltung (provet) durchgeführt und vom Bundesministerium für Wirtschaft und Technologie gefördert wird. Dem Beitrag liegt ein Vortrag zugrunde, den der Autor am 18.4.2000 in der Ritsumeikan University in Kyoto gehalten hat.

1) S. z.B. **Engels/Eimterbäumer,** Kommunikation und Recht 1998, 197f.

2) S. z.B. **Roßnagel,** Zeitschrift für Rechtspolitik 1997, 26 ff.; **Garstka,** Deutsches Verwaltungsblatt 1998, 987f.; **Hoffmann-Riem,** Datenschutz und Datensicherheit 1998, 686.

3) BVerfGE, 65, 1 (42 ff.).

Bundesdatenschutzgesetz immer weniger gewährleistet werden.

Genau zu diesem Zweck ist jedoch dieses Gesetz 1978 in Kraft getreten. Es sieht ein grundsätzliches Verbot vor, personenbezogene Daten zu verarbeiten. Ausnahmen bestehen nur, wenn der Betroffene einwilligt oder eine Rechtsvorschrift dies erlaubt. Die Verwendung der Daten ist an den Zweck, der in der Einwilligung oder in der Rechtsvorschrift genannt ist, gebunden. Der Betroffene hat das Recht auf Auskunft, Berichtigung, Sperrung oder Löschung. Die Datenverarbeiter sollen durch staatliche Behörden kontrolliert werden. Dieses alte Datenschutzrecht ist orientiert an einer Datei personenbezogener Daten, die von einer verantwortlichen datenverarbeitenden Stelle in einer zentralen Datenverarbeitungsanlage verarbeitet oder zu einer solchen übermittelt wird. Dieses Schutzkonzept ist in den 70er Jahren am Paradigma zentraler staatlicher Großrechner entwickelt worden. Soweit in dieser Form noch heute Daten verarbeitet werden, ist es weiterhin brauchbar. Soweit jedoch personenbezogene Daten in weltweiten Datennetzen von vielen Beteiligten ohne durchgreifende zentrale Kontrollmöglichkeiten verarbeitet werden, ist dieses Konzept überholt und durch neue Konzepte zu ergänzen oder zu ersetzen.

2. Das Teledienstedatenschutzgesetz als Antwort

Der Gesetzgeber hat die neuen Herausforderungen durch das Internet angenommen und in Form des Teledienstedatenschutzgesetz (TDDSG) eine Antwort gegeben.[4] Dieses Gesetz ist am 1. August 1997 in Kraft getreten.[5] Es ist ein bereichsspezifisches Gesetz, das auf Internetdienste Anwendung findet.

Das TDDSG will zum einen bewährte Grundsätze des Datenschutzes an die neuen technischen Entwicklungen anpassen und zum anderen erstmals neue Ansätze des Selbst- und Systemdatenschutzes umsetzen. Bewährte Grundsätze gelten nun auch für Internetdienste:

— Erlaubsnisvorbehalt: Datenverwendung nur auf der Grundlage einer Einwilligung oder einer Rechtsvorschrift (§ 3 Abs. 1 TDDSG). Neu ist, dass die Einwilligung nach § 3 Abs. 7 TDDSG) elektronisch erteilt werden kann.[6]

---

4) Das TDDS wurde durch ein Gutachten für einen „Datenschutz in Online-Multimediadiensten“ der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) 1996 unter Leitung des **Verfassers** vorbereitet - s. ‹www.iid.de/iukdg› und ‹www.provet.org/bib/mmge›.

5) Aufgrund der Verteilung der Gesetzgebungskompetenzen wurden die Internetdienste in Tele- und Mediendienste unterschieden. Den Datenschutz für Teledienste regelte der Bund im TDDSG, den Datenschutz für Mediendienste regelten die Länder in einem Mediendienste-Staatsvertrag - s. hierzu näher Roßnagel, in: ders. (Hrsg.), Recht der Multimedia-Dienste, Einführung, Rn. 13 ff. Da dessen Regelungen aufgrund der Abstimmung zwischen Bund und Ländern nahezu wortgleich sind, wird im folgenden der Einfachheit halber nur auf das TDDSG Bezug genommen.

6) S. hierzu auch **Bundesregierung,** BT-Drs. 14/1191, 13.

— Zweckbindung: Datenverwendung nur für den zugelassenen Zweck. Neu ist zum Beispiel das Gebot des § 4 Abs. 2 TDDSG, Nutzungsdaten nach der Nutzung sofort zu löschen, und das Verbot des § 4 Abs. 4 TDDSG, personenbezogene Profile zu erstellen.

— Transparenz: Unterrichtung des Betroffenen über die Datenverwendung und Recht auf Einsicht in die gespeicherten Daten. Neu ist zum Beispiel das in § 7 TDDSG gewährleistete Recht, beim Diensteanbieter kostenlos online Einsicht in die gespeicherten Daten nehmen zu können.[7]

3. Neue Datenschutzkonzepte

Es bleiben jedoch durch die technische Entwicklung und ihre weltweite Nutzung zwei Herausforderungen, die ergänzend neue Datenschutzkonzepte erforderlich machen:

Zum einen müssen neue Konzepte berücksichtigen, dass die dynamische Technikentwicklung — vermutlich noch umwälzender und rasanter — weitergehen wird. Daher genügen keine isolierten Antworten auf einzelne Sachprobleme. Benötigt werden vielmehr Strukturlösungen. Erforderlich ist, lernfähige Systeme zu etablieren, die auf sich ständig ändernde Herausforderungen immer wieder neue Antworten zu geben vermögen. Daher muss Datenschutz in die Technik eingebaut werden.

Zum anderen müssen neue Datenschutzkonzepte akzeptieren, dass die Regelungsmacht des Nationalstaats, auch der Europäischen Union, angesichts globaler Datennetze begrenzt ist. Zentrale staatliche Vorgaben zum Schutz der Persönlichkeit und ihre Kontrolle durch unabhängige staatliche Instanzen bleiben weiterhin notwendig, werden aber immer weniger den künftigen Aufgaben gerecht. Daher muss der Betroffene in die Lage versetzt werden, sich zu schützen.

Aufgrund dieser Herausforderungen sind drei neue Datenschutzkonzepte zu verfolgen:

3.1 Datenschutz durch Technik

Technik ist nicht nur als Gegner, sondern auch als Helfer des Datenschutzes anzusehen.[8] Je mehr der Datenschutz dem Einflußbereich des nationalen Gesetzgebers entschwindet, desto mehr muß Datenschutz weltweit wirksam werden. Dies ist mangels einer wirksamen Weltrechtsordnung nur dann möglich, wenn er in die Technik eingearbeitet ist. Dieser Weg bietet zwei Vorteile: Datenschutztechniken sind — im Gegensatz zu Datenschutzrecht — weltweit wirksam und Technikunternehmen sind — im Gegensatz zu Gesetzgebern — sehr schnell lernende Systeme.

---

7) S. hierzu näher **Schaar,** in: **Roßnagel** (Fn. 5), Kommentierung zu § 7 TDDSG.

8) S. z.B. **Information and Privacy Commisioner/Registratiekamer,** Privacy-Enhancing Technologies: The Path to Anonymity, 1995.

Beide Vorteile lassen sich nutzen, wenn es gelingt, für Datenschutztechnik einen Markt zu entwickeln.[9] Wenn sich Datenschutztechnik verkauft, wird sie sich ebenso dynamisch entwickeln wie neue technische Herausforderungen für den Datenschutz. Beispiele hierfür bietet der sich rasch entwickelnde Markt für Kryptograhphiesoftware und Sicherheitsdienstleistungen. Rechtliche Anforderungen stimulieren technische Lösungen und schaffen ihnen einen Markt, weil zumindest im Geltungsbereich eines Gesetzes alle, die personenbezogene Daten verwenden, Datenschutztechniken benötigen. Außerdem kann der Staat zu Unterstützung einer solchen Entwicklung passende Rahmenbedingungen setzen und entsprechende Forschungen fördern.

Technischer Datenschutz ist auch viel effektiver als rein rechtlicher Datenschutz. Was technisch verhindert wird oder unterbunden werden kann, muß nicht mehr verboten werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen eines Techniksystems nicht. Datenschutztechnik kann Kontrollen und Strafen und Strafen überflüssig machen.

Die §§ 3 bis 6 TDDSG geben erstmalig der Technikgestaltung durch den Diensteanbieter Ziele vor. Das Gesetz beschränkt sich nicht darauf, negative Technikfolgen zu mildern, sondern nimmt Einfluß auf die Gestaltung der Technik.[10]

3.2 Informationelle Selbstbestimmung durch Selbstdatenschutz

Aber auch Anforderungen an die Technik können nur im jeweiligen Staat wirken. Weiter jedoch wirken Regelungen, die Selbstdatenschutz ermöglichen.[11] Dem Betroffenen sollen eigene Instrumente in die Hand gegeben werden, seine informationelle Selbstbestimmung selbst zu schützen. Selbstdatenschutz kann durch technische Möglichkeiten der digitalen Signatur, des anonymen und pseudonymen Handelns, der Verschlüsselung, der Steganographie und viele weitere technische Hilfsmittel verbessert werden.[12] Dieser Ansatz verspricht zwei Vorteile:[13]

Die Betroffenen sind aus Eigeninteresse ebenfalls ständig lernende und sehr rasch

---

9) S. **Büllesbach,** Recht der Datenverarbeitung 1995, 1; **Büllesbach,** Recht der Datenverarbeitung 1997, 239.

10) S. **Lanfermann,** Recht der Datenverarbeitung 1998, 4; **Bizer,** in **Roßnagel** (Fn. 5), § 3 TDDSG, Rn. 15 ff.; **Schaar,** in **Roßnagel** (Fn 5), § 4 TDDSG, Rn. 43 ff.

11) S. zum Selbstdatenschutz z. B. **Roßnagel/Wedde/Hammer/Pordesch,** Digitalisierung der Grundrechte?, 1990, S. 220, 240 ff., 297 ff.; **provet** (Fn 4); **Trute,** Juristenzeitung 1998, 829; **Hoffmann-Riem,** in: Bäumler (Hrsg.), Der neue Datenschutz, 1998, 21 f.; **Schrader,** ebda., 206 ff.; **ders.,** DuD 1998, 128; **Engel-Flechsig,** in: **Lehmann** (Hrsg.), Rechtsgeschäfte im Netz—Electronic Commerce, 1999, 19 ff.; **Roßnagel,** Datenschutz und Datensicherheit 1999, 255f.

12) S. zu diesen Techniken z. B. Zwischenbericht der **Enquete-Kommission** „Zukunft der Medien in Wirtschaft und Gesellschaft" zu „Sicherheit und Schutz im Netz", BT-Drs. 13/11002, 94f.; **Konferenz der Datenschutzbeauftragten,** Datenschutzfreundliche Technologien, ‹www.datenschutz-berlin.de/to/datenfr.htm›.

13) S. hierzu auch **Roßnagel,** Datenschutz und Datensicherheit 1999, 255 ff.

reagierende Systeme. Daher ist es—wo dies möglich erscheint—sinnvoller, sie in die Lage zu versetzen, den ihnen jeweils wichtig erscheinenden Selbstschutz jederzeit realisieren zu können, als sie durch flächendeckende Vorgaben zwangsweise zu beglücken. Außerdem wirkt auch dieser Ansatz weltweit: Die Selbstschutztechniken können grundsätzlich bei allen Kontakten in globalen Netzen Anwendung finden.

3.2.1 Beispiel P3P

Selbstbestimmung setzt Transparenz über die Datenverarbeitung voraus. Hier könnte der Datenschutzstandard „Platform for Privacy Preferences Project (P3P)" des WWW-Konsortiums helfen.[14] P3P ermöglicht die formalisierte und maschinenlesbare Beschreibung von Datenschutzverhalten. Ein Anbieter formuliert seine „Policy" und verweist im ersten „Response" auf eine Web-Anfrage auf diese. Mit Hilfe einer P3P-Nutzerkomponente formuliert ein Nutzer seine Nutzerpräferenzen („Preferences"), speichert diese lokal bei sich ab vergleicht diese mit heruntergeladenen „Policies" der Anbieter. Entsprechend dem Ergebnis initiiert die Nutzerkomponente das weitere Vorgehen — weitere Nutzung der Web-Seite oder Verlassen der Web-Seite—entweder automatisch oder nach lokaler Interaktion mit dem Nutzer. Ein Nutzer kann mit Hilfe einer P3P-Nutzerkomponente dafür sorgen, dass er nur solche Dienste in Anspruch nimmt, die seinen Datenschutzanforderungen genügen. Eine Anwendung von P3P wird in der Bewertung der Datenschutzfreundlichkeit von Telediensten („Rating") liegen. Formale Beschreibungen ermöglichen automatische (oder wenigstens halb-automatische) Auswertungen. Dadurch können Teledienste flächendeckend ausgewertet werden. Außerdem wird ein Vergleich zwischen verschiedenen Telediensten durchschaubarer.[15] „Infomediaries", neu entstehende Unternehmen, die als Datentreuhänder Datenschutzdienste für Nutzer anbieten, dürften deshalb P3P am intensivsten nutzen.[16]

3.2.2 Beispiel Pseudonymität

Besondere Bedeutung für den Selbstdatenschutz kommt dem Konzept pseudonymen Handelns zu.[17] Auf dieses soll daher etwas näher eingegangen werden. Die Verarbeitung

14) The Platform for Privacy Preferences 1.0 (P3P1.0) Specification; W3C Working Draft, 2.11.1999. Previous Version: Platform for Privacy Preferences (P3P) Specification, W3C Working Draft 26.8.1999; s. auch P3P Guiding Principles, W3C Note 21.7.1998, www.w3.org/p3p.

15) S. hierzu näher **Grimm/Roßnagel,** in: **Kubicek/Braczyk/Klumpp/Roßnagel** (Hrsg.), Golbal@Home, Jahrbuch für Telekommunikation und Gesellschaft 2000, 293 ff.

16) S. z.B. www.digitalme.com; www.enonimous.com; www.privaseek.com; www.privacybank.com; **Hagel III/Singer,** Net Worth. The Emerging Role of the Infomediary in the Race for Costumer Information, 1999.

17) Zur Forderung nach Anonymität und Pseudonymität s. z.B. **Registratiekamer/Information & Privacy Commissioner,** Privacy-enhancing Technologies: The path to Anonymity, 1995; **Rat für Forschung, Technologie und Innovation,** Informationsgesellschaft — Chancen, Innovationen und Herausforderungen, 1995, 2.5 Empfehlung 23, www.technologierat.de/vdi/frames/report95.htm; **Art. 29-Datenschutzarbeitsgruppe,** Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet, www.datenschutz-berlin.de/doc/eu/gruppe29/bbmem-de.htm; **Enquete**-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft" (Fn. 12), 94 f; **Simitis** in: Festschrift für Kübler, 1997, 285 ff.

„Datensparsamkeit". Anonymität ist jedoch nicht immer erwünscht oder sinnvoll.[18] Wenn der Personenbezug entfällt, kann leicht die Verantwortlichkeit für persönliches Handeln verloren gehen. Außerdem ist es in vielen Lebenssituationen erforderlich, Personen identifizieren zu können, etwa als Vertragspartner, als Amtsinhaber oder Träger einer Berechtigung.

Um sowohl Datensparsamkeit als auch Identifizierbarkeit einer Person zu ermöglichen, kann auf das Konzept pseudonymen Handelns zurückgegriffen werden.[19] Denn es vermag den Zielkonflikt zwischen notwendiger Identifizierung des Betroffenen und dessen Wunsch nach Anonymität[20] zu vermeiden, indem es zwischen Regelfall (keine Identifizierung) und Ausnahmefall (Identifizierungsmöglichkeit) unterscheidet. „Pseudonym" kommt aus dem Griechischen (pseudónymos „fälschlich so genannt") und bedeutet nach allgemeinem Verständnis so viel wie „erfundener Name", „fingierter Name" oder „Deckname".[21] Der Entwurf zu § 3 Abs. 6a BDSG-E definiert[22] „Pseudonymisieren" als „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren". Indem der Betroffene in verschiedenen Situationen unter Pseudonym (Kennzeichen) handelt, kann er verhindern, dass er bei jedem, der davon erfährt, Datenspuren hinterläßt, die zu ihm führen und die gegen seinen Willen gesammelt, weiterverarbeitet und weitergeben werden können. Eine vergleichbare Wirkung kann erzielt werden, wenn bei personenbezogenen Daten nachträglich die identifizierenden Teile durch Pseudonyme ersetzt werden. Da das Pseudonym einer bestimmten Person zugeordnet wurde, kann diese jedoch—im Gegensatz zur Verwendung anonymisierter Daten—über die Zuordnungsregel identifiziert werden. Gegenüber pseudonym Handelnden besteht somit die Möglichkeit, sie zur Verantwortung zu ziehen, wenn sie etwa ihre Vertragspflichten nicht erfüllen oder ihre Berechtigungen überschreiten.

Bei richtiger Handhabung können sich Pseudonyme als ein wichtiges Instrument zur Vermeidung unerfreulicher Konfliktlagen erweisen, bei denen in der Vergangenheit öfter wichtige andere Interessen wie Forschung, Planung, Statistik, Marketing oder Öffentlich-

---

18) S. zu den Nachteilen von Anonymität **Caronni,** Datenschutz und Datensicherheit 1998, 623 ff.

19) S. hierzu auch **Roßnagel** in: Festschrift für Podlech, 1994, S. 245f.; **provet/GMD,** Die Simulationsstudie Rechtspflege, 1994, 210 ff.; BT-Drs. 13/7385, 23; **Roßnagel,** in: ders. (Fn. 5), Einführung, Rn. 61f.; **Bizer,** in: **Roßnagel** (Fußn. 5), § 3 TDDSG, Rn. 175 ff.

20) Zur datenschutzerechtlichen Bedeutung von Anonymität s. **Simitis** (Fn. 17), 309; zu Anonymitätstechniken s. **Borking,** Datenschutz und Datensicherheit 1996, 654.; **Arbeitskreis Technik** der Konferenz der Datenschutzbeauftragte, Datenschutz und Datensicherheit 1997, 709 ff.; **Federrath/Pfitzmann,** Datenschutz und Datensicherheit 1998, 628 ff.; **Demuth/Rieke,** Datenschutz und Datensicherheit 1998, 623 ff.; **Roessler,** Datenschutz und Datensicherheit 1998, 619 ff.

21) Brockhaus—Die Enzyklopädie, 20. Aufl. 1996; **Bizer/Bleumer,** Datenschutz und Datensicherheit 1997, 46.

22) § 4 Abs. 1 TDDSG definiert pseudonyme Nutzung nicht. Zur Forderung nach einer gesetzlichen Definition s. Bundesregierung, BT-Drs. 14/1191, 15.

keitsarbeit gegen den Datenschutz ins Feld geführt wurden und umgekehrt.[23] Dies gilt insbesondere für den Electronic Commerce. Bisher mogelt man sich dort um das Problem des Datenschutzes noch eher herum. Die Folge ist, daß die Anbieter heimlich personenbezogene Daten sammeln, und zwar mehr als sie für ein Geschäft unmittelbar brauchen, während die Kunden systematisch über alle die Daten lügen, die für das Geschäftes nicht unbedingt erforderlich sind. Die Datensammlungen der Firmen quellen über von 90jährigen „Donald Ducks" mit 10 Kindern, die in „Bahnhofstraßen" wohnen und phantasievolle Email-Adressen und Telefonnummern besitzen. Die Firmen haben viel zu viele nutzlose Daten. Die Kunden trauen den Anbitern nicht, mit ihren richtigen Daten korrekt umzugehen. Pseudonyme könnten die Kunden veranlassen, richtige Zusatzangaben zu machen, und den Anbietern ermöglichen, zwar keine personenbezogenen, aber ansonsten wahre Kundenprofile zu erstellen.

Mittels der Vergabe von Pseudonymen sollen personenbezogene Daten derart verändert werden, daß sie ohne Kenntnis der jeweiligen Zuordnungsregel nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, für den Ausnahmefall aber mittels der Zuordnungsregel die Identifizierung der Person ermöglichen.[24] Der datenschutzfreundliche Effekt der Pseudonymisierung wird gegenüber den Datenverwendern erreicht, die keinen Zugriff auf die jeweilige Zuordnungsfunktion haben. Ihnen ist daher die Zuordnung von Kennzeichen und Identität des Namensträgers nicht ohne weiteres möglich. Dagegen ist für den Kenner der Zuordnungsregel die Zuordnung einfach, die Daten sind für ihn personenbeziehbar. Fehlt Dritten die Zuordnungsregel, besteht hinsichtlich der Abgrenzung zu personenbeziehbaren Daten kein Unterschied zu anonymen Daten.[25]

Hier kann die Unterscheidung von Pseudonymen nach dem Inhaber der Zuordnungsregel rechtlich bedeutsam sein. Es sind grundsätzlich drei Arten von Pseudonymen zu unterscheiden:

Werden Pseudonyme ausschließlich vom **Betroffenen** selbst vergeben und nicht mit Identitätsdaten gleichzeitig verwendet oder gespeichert, kann der Personenbezug auch nur vom Betroffenen selbst hergestellt werden.[26] Ein vom Nutzer selbst vergebenes

---

23) S. Begründung zu § 10 Abs. 6 und § 22 Landesdatenschutzgesetz Schleswig-Holstein, LT-Drs. 14/1738, 55f., 67f.

24) Ähnlich § 2 Abs. 5 Landesdatenschutzgesetz Schleswig-Holstein und § 3 Abs. 3 Nr. 2 Landesdatenschutzgesetz Brandenburg. S. auch die Formulierung des AK Technik **(Fn. 20), Datenschutz und Datensicherheit 1997, 711,** und des AK „**Datenschutz-Audit Multimedia**", Datenschutz und Datensicherheit 1999, 290.

25) Ebenso Begründung zu § 22 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein, LT-Drs. 14/1738, 66f.

26) Der **AK Technik** (Fn. 20), Datenschutz und Datensicherheit 1997, 711 spricht von selbstgenerierten Pseudonymen.

Pseudonym ist beispielsweise die frei gewählte Benutzer-ID, die vor der Inanspruchnahme eines Internet-Angebots angegeben werden muß. Für den datenverarbeitenden Anbieter weisen Daten, die ausschließlich in Verbindung mit einem solchen Pseudonym stehen, grundsätzlich keinen Personenbezug auf. In diesem Fall hat es grundsätzlich nur der Nutzer in der Hand, die Identität eines Pseudonyms preiszugeben.

Die Pseudonyme können von einem **vertrauenswürdigen Dritten** vergeben werden, der allein über die Zuordnungsregel verfügt.[27] Diese Organisationsform sieht das SigG vor. Jeder, der dies möchte, kann sich nach § 7 I SigG Signaturschlüssel auf andere Namen als seinen eigenen als Pseudonyme zertifizieren lassen.[28] Zusätzlich kann er im Zertifikat oder in einem Attributzertifikat nach § 7 II und III SigG Vollmachten, Berufszulassungen, Amtseigenschaften sowie sonstige Berechtigungen bestätigen lassen und damit im Rechtsverkehr qualifiziert auftreten, ohne seine Identität aufdecken zu müssen.[29] In dieser Alternative kennt nicht nur der Betroffene, sondern auch ein Dritter die Identität des Pseudonyms. Allerdings besteht typischerweise eine organisatorische Trennung zwischen dem Inhaber der Zuordnungsregel und dem potentiellen Datenverwender. So bezieht zum Beispiel der Betroffene sein pseudonymes Zertifikat von einer Zertifizierungsstelle und verwendet es beim Interneteinkauf gegenüber verschiedenen Anbietern, die grundsätzlich keinen Zugriff auf die Zuordnungsregel haben.

Die dritte Möglichkeit besteht darin, daß der ursprüngliche **Datenverwender** das Pseudonym vergibt und über die Zuordnungsregel verfügt. Das Pseudonym schützt dann nicht ihm gegenüber, aber gegenüber allen Dritten. Beispielsweise könnte der Betreiber einer Internet-Mall den virtuellen Besucher bei seiner Anmeldung mit Namen und Adresse für den „Einkaufsbummel“ ein Pseudonym zuweisen, unter dem er in den einzelnen Internet-Shops einkaufen kann. Diese erfahren nicht die Identität dessen, der sich für ihre Produkte interessiert. Der Mall-Betreiber kennt aber die Identität des Käufers und kann ihm Rechnung und Waren an seine Adresse senden. Wie in der zweiten Alternative hat es der Betroffene nicht mehr allein in der Hand, die Identität des Pseudonyms zu wahren. Vielmehr teilt er dieses Geheimnis mit einem anderen, der es selbständig aufdecken kann. Im Unterschied zur zweiten Alternative hat der Kenner der Zuordnungsregel ein eigenes Datenverwendungsinteresse und kann trotz Pseudonym die Daten personenbezogen verwenden. Ein weiteres Beispiel stellen dynamische vergebene IP-Nummern dar. Dem

27) Eine solche Möglichkeit sieht auch der **AK Technik** (Fn. 20), Datenschutz und Datensicherheit 1997, 711 für die von ihm sogenannten Referenz-Pseudonyme vor. S. hierzu auch die amtliche Begründung zum TDDSG, BT-Drs. 13/7385, 23. Bei dieser Art von Pseudonymen kann der Personenbezug nur über entsprechende Referenzlisten hergestellt werden, die vorzugsweise räumlich und organisatorisch getrennt von den pseudonymisierten Daten in einer Vertrauensstelle zu speichern sind.

28) S. hierzu **Roßnagel,** in: **ders.** (Fn. 5), § 7 SigG, Rn. 34f.

29) S. zu Pseudonymen mit qualifizierendem Zertifikat **Roßnagel,** in: **ders.** (Fn. 5), § 7 SigG, Rn. 62f.; **provet/GMD** (Fn. 19), 213 ff.; **Pordesch,** in: **Roßnagel/Haux/Herzog** (Hrsg.), Mobile und sichere Kommunikation im Gesundheitswesen, 1999, 156 ff.

Access-Provider sind die personenbezogenen Daten des Nutzers zwar bekannt, der Nutzer agiert gegenüber den angewählten Anbieter-Servern jedoch unter einer—innerhalb des IP-Adressenraums des Providers — wechselnden IP-Adresse, die somit temporär sein Pseudonym ist. Für Dritte kann ein Personenbezug über IP-Adressen nicht hergestellt werden. Sie können dies nur dann, wenn sie mit dem Access-Provider, der über die Zuordnungsregel verfügt, zusammenarbeiten.[30]

§ 4 Abs. 1 TDDSG ermöglichen alle drei Alternativen. Er fordert von jedem Diensteanbieter, dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Dies deutet in erster Linie auf die dritte Alternative hin. Doch muss der Diensteanbieter die Pseudonyme nicht selbst vergeben und verwalten, sondern er könnte ebenso pseudonyme Zertifikate einer Zertifizierungsstelle oder selbstgenerierte Pseudonyme akzeptieren.

Mit dieser Regelung soll zugleich dem Anbieter von Multimediadiensten ein Anreiz geboten werden, diese datenschutzfreundlichen Methoden zu nutzen. Durch die Pseudonymisierung wird den Daten ihr Personenbezug praktisch genommen. Dem Anbieter wird die Chance eröffnet, sich dadurch dem Anwendungsbereich der Datenschutzgesetze zu entziehen.[31] Die Fortgeltung der Anbieterpflichten trotz praktischem Ausschluß des Personenbezugs wäre mit dem Sinn und Zweck der Vorschriften nicht zu vereinbaren.[32] Umgekehrt gibt gerade die Nichtgeltung der Datenschutzanforderungen den Anreiz, das Ziel der Einsparung personenbezogener Daten durch die Verwendung anonymer oder pseudonymer Daten umzusetzen. Wer nur solche Daten verwendet, ist von den folgenden Anforderungen befreit:

- Er unterliegt nicht dem generellen Verbot der Datenverarbeitung aus § 4 Abs. 1 BDSG, § 3 Abs. 1 TDDSG. Er ist weder an spezielle Erlaubnistatbestände gebunden noch muß er eine Einwilligung für die Datenverwendung einholen.
- Für pseudonyme Daten gilt keine Zweckbindung. Insbesondere müssen nicht die besonderen Beschränkungen für die Übermittlung von Daten beachtet werden.
- Er muß den Nutzer vor der Datenerhebung nicht nach § 3 Abs. 5 TDDSG unterrichten.
- Er unterliegt nicht spezifischen oder sich aus dem Erforderlichkeitsgrundsatz ergebenden Löschungspflichten.

---

30) **Schaar/Schulz,** in: **Roßnagel** (Fn. 7), § 4 TDDSG, Rn. 49.

31) S. Begründung zu § 4 TDDSG, BT-Drs. 13/7385, 23; s. auch **Engel-Flechsig,** Recht der Datenverarbeitung 1997, 65; **ders.** (Fn. 11), 21; **Schulz/Schaar,** in: **Roßnagel** (Fn. 5). § 4 TDDSG, Rn. 45; **Bäumler,** Datenschutz und Datensicherheit 1999, 260.

32) **Gola/Schomerus,** Kommentar zum BDSG, § 3 Anm. 14.2; § 40 Anm 2.3; **Simitis,** in: **Simitis/Dammann/Geiger/Mallmann/Walz,** Kommentar zum BDSG, § 40 Rn.60. Für eine rechtliche Gleichstellung auch der **Landesbeauftragte für Datenschutz Schleswig-Holstein,** LT-Drs. 14/1738, 40; **Bizer,** in: **Roßnagel** (Fn. 5), § 3 TDDSG, Rn. 69, 168.

- Ihn trifft nicht die sich § 35 BDSG ergebende Pflicht zur Berichtigung, Sperrung und Löschung.
- Er unterliegt nicht dem grundsätzlichen Verbot der Profilbildung nach § 4 Abs. 4 TDDSG und muß auch der Forderung nach Vertraulichkeit und getrennter Datenverarbeitung nach § 4 Abs. 2 Nr. 3 und 4 TDDSG nicht nachkommen.
- Ihn trifft keine Pflicht zur technisch-organisatorischen Sicherung der Daten.
- Schließlich entfällt auch die nach § 32 BDSG für private Datenverarbeiter vorgesehene Meldepflicht.
- Maßnahmen der Datenschutzkontrolle finden nur soweit statt, bis die Aufsichtsbehörden sich davon überzeugt haben, daß es sich nicht um personenbeziehbare Daten handelt.

Bei der Verwendung von Pseudonymen verbleiben jedoch gewisse Datenschutzrisiken. Werden die gleichen Pseudonyme über längere Zeit genutzt, besteht die Möglichkeit, das die Informationen über diese Pseudonyme verkettet werden. So können Datensammlungen bis hin zu umfassenden Profilen unter einem Pseudonym entstehen. Wird das Pseudonym aufgedeckt, werden alle diese Daten der betroffenen Person auf einen Schlag zuordenbar. Das andere Risiko besteht darin, daß die Zuordnungsregel auch bisher Unwissenden bekannt wird. Dies kann ungewollt etwa dadurch erfolgen, dass der Kenner der Zuordnungsregel unbemerkt Wissen preisgibt, das den Empfänger zur Aufdeckung des Pseudonyms befähigt. Neben der oben angeführten Gefahr einer zufälligen Aufdeckung spielt für Pseudonyme vor allem die gewollte, freiwillige Aufdeckung eine entscheidende Rolle.[33)]

Der Vorteil des Einsatzes von Pseudonymen gegenüber anonymem Handeln besteht auch oder gerade in der Möglichkeit zur bedarfsgerechten Aufdeckung des Pseudonyms in Konfliktfällen. Dies kann zum einen—beispielsweise bei Reklamationen —im Interesse des Pseudonymträgers liegen. Aber auch der andere Partner, der mit einem pseudonym handelnden kooperiert, kann ein berechtigtes Interesse an einer Aufdeckung des Pseudonyms haben. So kann bei Rechtsgeschäften, in denen der Leistungsaustausch nicht zur gleichen Zeit stattfindet, sondern eine Partei vorleistet, dieser nicht zugemutet werden, die Leistung gegenüber einem anonym Handelnden zu erbringen. Vielmehr muss sie die Möglichkeit haben, den Vertragspartner im Fall der Nicht-oder Schlechterfüllung zur Rechenschaft zu ziehen und mögliche Gewährleistungsansprüche durchzusetzen. In diesem Fall kann mit Hilfe von Pseudonymen selbstbestimmter Datenschutz gewährleistet und den Interessen des Vorleistenden Rechnung getragen werden, wenn im Streitfall durch ein geordnetes Aufdeckungsverfahren ihm gegenüber die Aufdeckung des Pseudonyms garantiert ist. Ist der Vertragspartner nur an der Erfüllung des Zahlungsanspruchs interessiert, kann sein Interesse durch einen Garantiebetrag für das Pseudonym befriedigt

33) S. hierzu näher **Roßnagel/Scholz,** Multimedia und Recht 2000, Heft 7, im Erscheinen.

werden, dessen Auszahlung eine Aufdeckung überflüssig macht.[34]

Durch die Aufdeckung werden alle zu einem Pseudonym gespeicherten Daten zu personenbezogenen Daten. Dann gelten von diesem Zeitpunkt an die Regeln des Datenschutzrechts, aber viele Schutzmaßnahmen, die das Datenschutzrecht für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten fordert, können dann nicht mehr sinnvoll nachgeholt werden.

Die Folgen einer nachträglichen Aufdeckung sind sowohl für den Datenverwender als auch vor allem für den Betroffenen sehr unbefriedigend.[35] Um ausreichenden Schutz für die informationelle Selbstbestimmung zu gewährleisten, sind datenschutzrechtliche Regelungen notwendig, die Vorsorge gegen die Aufdeckungsrisiken und ihre Folgen für Daten bieten, die keine personenbezogenen Daten sind, aber zu solchen werden können.[36] Notwendig sind daher Vorsorgeregelungen zur

- Information des Betroffenen. Er muß wissen, welche Maßnahmen er ergreifen kann oder vermeiden muß, um eine Beseitigung der Pseudonymität zu verhindern. Nachträglich ist zumindest erforderlich, daß der Betroffene Informationen über ihre Verwendung der pseudonymen Daten erhalten kann.[37]
- Sicherung der Pseudonymitätseigenschaft: Es sind Vorsorgemaßnahmen notwendig, die zum einen die Wahrscheinlichkeit ihres Personenbezugs vermindern und zum anderen das Schadenspotential einer Aufdeckung reduzieren.[38]

Bisher fehlen im deutschen Recht jedoch Regelungen für ein Aufdeckungsverfahren für Private.[39] § 12 Abs. 2 Signaturgesetz sieht nur einen Aufdeckungsanspruch für Sicherheitsbehörden und Geheimdienste vor. Würde der Aufdeckungsanspruch und ein geeignetes Aufdeckungsverfahren in der anstehenden Novelle des TDDSG geregelt, wäre das Konzept pseudonymen Handelns ein neues und erfolgversprechendes Instrument des Selbstdatenschutzes.

3.3 Datensparsamkeit durch Systemdatenschutz

An die Diensteanbieter gewendet fordert das TDDSG in § 3 Abs. 4 als neues Datenschutzziel Datenvermeidung oder Datensparsamkeit. Es geht von der Erkenntnis aus, dass der beste Datenschutz dann gewährleistet werden kann, wenn gar keine

---

34) S. **Pfitzmann/Waidner/Pfitzmann,** Datenschutz und Datensicherheit 1990, 305 ff.; **Pfitzmann,** Datenschutz und Datensicherheit 1999, 406.

35) S. hierzu genauer **Roßnagel/Scholz,** Multimedia und Recht 2000, Heft 7, im Erscheinen.

36) S. hierzu z.B. **Bizer,** Forschungsfreiheit und informationelle Selbstbestimmung, 1992, 153 ff.; BVerfGE 65, 1 (49); BVerfG, Neue Juristische Wochenschrift 1987, 2805 (2806).

37) Die präventive Transparenz ist bereits in § 4 Abs. 1 Satz 2 TDDSG angelegt, die nachträgliche Transparenz durch § 7 TDDSG geboten.

38) § 4 Abs. 4 Satz 2 TDDSG sieht für unter Pseudonym erstellte Nutzungsprofile eine solche Sicherungsregel bereits vor.

39) S. hierzu bereits **Roßnagel,** Datenschutz und Datensicherheit 1997, 75 ff.

personenbezogenen Daten entstehen. Dabei soll bereits durch die Gestaltung der Systemstrukturen, in denen personenbezogene Daten erhoben und verarbeitet werden können, die Erhebung und Verwendung personenbezogener Daten vermieden und die Selbstbestimmung der Nutzer sichergestellt werden.[40]

Systemdatenschutz fordert von den Diensteanbietern, ihre Datenverarbeitungsstrukturen daraufhin zu überprüfen, ob sie ihre Angebote so umstellen können, dass weniger personenbezogene Daten entstehen.[41] So erspart ein Leistungsangebot nach Zeittakt, Inhalte zu speichern, und ein Leistungsangebot nach „Flatrates", Zeittakte zu speichern. Bei Gütern, die elektronisch bestellt, aber physisch ausgeliefert werden, könnte eine datenaufteilende Systemorganisation erübrigen, dass die Verkäufer Name und Anschrift des Käufers, der eingeschaltete Auslieferservice Ware und Preis kennen müssen. Entscheidend für den Systemdatenschutz dürfte die Wahl von Bezahlverfahren im Internet sein. Bei sicherem zeitgleichem Austausch von Leistung und Gegenleistung kann dies technisch ebenso anonym erfolgen wie im Kaufhaus oder auf dem Marktplatz. Dies kann bei Zahlungen mit Kreditkarten zum Beispiel durch den „Secure Transaction Standard" (SET) erreicht werden, in dessen Version mit drei Schlüsselpaaren der Käufer gegenüber dem Verkäufer nur als Pseudonym auftritt.[42] Um Selbstdatenschutz zu ermöglichen, fordert § 4 Abs. 1 TDDSG von jedem Diesteanbieter, dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.[43]

Systemdatenschutz ist nur gegenüber Stellen in Deutschland durchzusetzen. Gegenüber Anbietern von Dienstleistungen weltweit kann nur das Vorbild nachahmend wirken, wenn aus datenschutzkonformen Lösungen ein Wettbewerbsvorteil erwächst. Systemdatenschutz kann aber in Datenschutztechnik eingehen und über diese weltweit angeboten werden.

---

40) Grundlegend zum Systemdatenschutz **Podlech,** in: Festschrift für Grüner, 1982, 451 ff.; s. auch **Roßnagel** (Fn. 19), 236 ff.; **ders.,** Zeitschrift für Rechtspolitik 1997, 29; **ders.,** Datenschutz und Datensicherheit 1999, 256; **Engel-Flechsig,** Datenschutz und Datensicherheit 1997, 13 f.; **Büllesbach/Garstka,** in: Müller/Pfitzmann (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Band I, 1997, 383 ff.; **Hoffmann-Riem,** Archiv des öffentlichen Rechts 1998, 535; **Kloepfer,** 62. Deutscher Juristentag 1998, D, 98f.; **Garstka,** Deutsches Verwaltungsblatt 1998, 988; **Trute,** Juristenzeitung 1998, 827f.; zum Datenschutz durch Technikgestaltung s. z.B. **Bäumler,** Datenschutz und Datensicherheit 1997, 448 ff.; **ders.,** Recht der Datenverarbeitung 1999, 7; Bizer, in: **Bäumler** (Hrsg.), Datenschutzgesetze der dritten Generation, 1999, 28 ff.

41) Bundesregierung, BT-Drs. 14/1191, 13; s. auch **Bizer,** in: **Roßnagel** (Fn. 5), § 3 TDDSG, Rn. 131 ff.

42) S. hierzu SET, Secure Electronic Transaction Specification, V. 1.0, 31.5.1997, http://www.setco.org/.

43) Zu diesen Begriffen s. **Schaar/Schulz,** in: **Roßnagel** (Fn. 5), § 3 TDDSG, Rn. 44 ff.

4. Umsetzungsprobleme und Lösungsansätze

Das TDDSG war für den Gesetzgeber ein Experiment. Deswegen hat er beschlossen, nach zwei Jahren eine Evaluierung durchzuführen. Die Evaluierung ist im letzten Sommer erfolgt und hat zwei wichtige Ergebnisse gebracht.[44] Das erste Ergebnis ist die Feststellung, dass sich das TDDSG grundsätzlich bewährt hat. Das zweite Ergebnis war jedoch die Feststellung, dass die Anforderungen bei einem Teil der betroffenen Wirtschaft, insbesondere bei kleinen und mittleren Unternehmen, noch nicht ausreichend bekannt sind oder nicht beachtet werden. Auch waren diese über die technischen Möglichkeiten nicht ausreichend unterrichtet.[45]

Dieses Vollzugsdefizit ist ein grundsätzliches Problem eines eher persuasiven Rechts.[46] Um den Vorwurf einer Überregulierung zu vermeiden, wurde im TDDSG auf Strafvorschriften verzichtet.[47] Dies mag im Rahmen eines partnerschaftlichen Verhältnisses zwischen Staat, Bürgern und Unternehmen sinnvoll sein, erfordert aber ergänzende Maßnahmen. Ich sehe zwei Ansätze für die Reduzierung des Vollzugsdefizits.

4.1 Anreiz: Datenschutzaudit

Zum einen müssen Mechanismen genutzt werden, die den Handlungslogiken der Unternehmen stärker entgegenkommen. Einen solchen Mechanismus bietet das Datenschutzaudit: Durch die abgesicherte Möglichkeit, mit seinen Datenschutzanstrengungen werben zu können, soll der Datenverarbeiter veranlaßt werden, freiwillig ein Datenschutzmanagementsystem zu errichten, das zu einer kontinuierlichen Verbesserung des Datenschutzes beiträgt.[48] Nach einer externen Überprüfung der Datenschutzmaßnahmen kann das Unternehmen ein Datenschutzauditzeichen für seine Werbung benutzen.[49]

Das Ziel einer kontinuierlichen Verbesserung kann das Datenschutzaudit nur erreichen, wenn es als ein Lernsystem verstanden wird.[50] In regelmäßigen Abständen

---

44) S. zur Evaluierung auch **Schulz,** in: **Kubicek** et al. (Hrsg.), Multimedia@Verwaltung. Jahrbuch Telekommunikation und Gesellschaft 1999, 202; **Roßnagel,** Datenschutz und Datensicherheit 1999, 253; **Bäumler,** Datenschutz und Datensicherheit 1999, 258; **Büllesbach,** Datenschutz und Datensicherheit 1999, 263.

45) Bundesregierung, BT-Drs. 14/1191, 14 ff.; **Bäumler,** Datenschutz und Datensicherheit 1999, 262, **Wolters,** Datenschutz und Datensicherheit 1999, 277, 280; Bundesbeauftragter für den Datenschutz, 17. Tatigkeitsbericht, 1999, 146; **Tettenborn,** Multimedia und Recht 1999, 519. **Roßnagel,** Datenschutz und Datensicherheit 1999, 257; **Büllesbach,** Datenschutz und Datensicherheit 1999, 265; **Grimm/Löhndorf/Scholz,** Datenschutz und Datensicherheit 1999, 273.

46) S. hierzu **Roßnagel,** Neue Zeitschrift für Verwaltungsrecht 2000, 266 ff.

47) Dies soll in der geplanten Novelle zum TDDSG geändert werden. Dort sind in § 9 Bußgeldvorschriften vorgesehen-**Bundesregierung,** BT-Drs. 14/1191, 16.

48) Die Einhaltung des Datenschutzrechts ist selbstverständlich und keine Auszeichnung wert.

49) S. hierzu **Roßnagel,** Datenschutzaudit-Konzeption, Durchführung, gesetzliche Regelung, 2000.

überprüft die datenverarbeitende Stelle die Umsetzung ihrer Zielsetzungen und schreibt diese fort. In die Fortschreibung gehen positive und negative Erfahrungen mit der Umsetzung bisheriger Datenschutzmaßnahmen ein, die in reflektierter Form die nächsten Verbesserungsschritte bestimmen. Mit der Strukturierung eines solchen Lernprozesses würde in den Datenschutz ein neues förderliches Element eingefügt. Es geht nicht darum, einzelnen Lösungen auszuzeichnen, sondern die Fähigkeit eines Managementsystems, in einer sich ständig sehr schnell ändernden Welt immer wieder Lösungen für neue Herausforderungen zu finden.

Der Entwurf eines Rahmengesetzes für das Datenschutzaudit wurde im Auftrag der Bundesregierung im Sommer 1999 erstellt.[51] Die Bundesregierung beabsichtigt, auf der Grundlage dieses Vorschlags ein Datenschutzauditgesetz zu erlassen.[52]

4.2 Vorbild: Beispiel DASIT

Zum anderen muss die Effektivität der Gesetze durch umfassende Begleitmaßnahmen für die Aufklärung und Überzeugung gefördert werden. Die positiven Wirkungen des TDDSG werden nur zu erwarten sein, wenn sein Inhalt, vor allem aber Möglichkeiten. ihn umzusetzen, ausreichend bekanntgemacht werden. Soll das TDDSG sich nicht nur als symbolisches Recht erweisen, müssen mehr Anstrengungen für Pilot-und Demonstrationslösungen unternommen werden.

Solche Pilot-und Demonstrationslösungen sollen für das elektronischen Einkaufen und Bezahlen im Internet in dem Forschungsprojekt „Datenschutz in Telediensten (DASIT)“ erarbeitet werden. Das Projekt wird von der DG Bank, Deutsche Genossenschaftsbank AG, dem GMD—Forschungszentrum Informationstechnik GmbH und der Projektgruppe verfassungsverträgliche Technikgestaltung der Universität Kassel von Oktober 1998 bis März 2001 durchgeführt. Es wird vom Bundesministerium für Wirtschaft und Technologie finanziert. In dem Projekt wird am organisatorischen Beispiel einer „Electronic Mall“ und am technischen Beispiel eines „Electronic Wallets“ gezeigt, wie die Anforderungen des TDDSG in der Praxis umgesetzt werden können. Für die Mall wird untersucht, wo vom Anbieten der Waren bis zu deren Auslieferung und Bezahlung personenbezogene Daten eingespart werden können. Für das Wallet wird gezeigt, wie mit Hilfe des Standards SET anonym und pseudonym eingekauft und bezahlt werden kann. Außerdem wird das Wallet

---

50) Hier liegt ein entscheidender Unterschied zum Privacy Mark System des JIPDEC und der CBA in Japan.

51) Das Gutachten hierzu ist in **Roßnagel** (Fn. 49) enthalten.

52) **Bundesregierung,** BT-Drs. 14/1191, S. 14 und **Bundesregierung,** Aktionsprogramm „Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts, BT-Drs. 14/1776=BR-Drs. 551/99, abrufbar unter ‹http://www.bmwi.de›. Kap. 3.4; **Tettenborn,** Multimedia und Recht 1999, 520.

53) S. hierzu **Grimm/Löhndorf/Scholz,** Datenschutz und Datensicherheit 1999, 272; **Grimm/Löhndorf/Roßnagel,** E-Commerce meets E-Privacy, in: **Bäumler** (Hrsg.), Datenschutz im Electronic Commerce, 2000, im Erscheinen.

auch den Nutzer unterstützen, seine Datenschutzrechte wahrzunehmen. In ihm werden Möglichkeiten datenschutzorientierter Kommunikation zwischen Client und Server nach dem P3P-Standard realisiert. Außerdem bietet das Wallet die Möglichkeit, elektronisch einzuwilligen, die Einwilligung zu widerrufen, online die zur eigenen Person gespeicherten Daten einzusehen und online Forderungen nach Berichtigung, Sperrung oder Löschung der Daten zu stellen. Diese Lösungen sollen ab Sommer in einem Feldversuch getestet werden.[33)]

5. Ausblick

Insgesamt, so kann ich meine Ausführungen zusammenfassen, scheint mir die Bundesrepublik Deutschland auf dem richtigen Weg zu sein, einen zukunftsweisenden Datenschutz im Internet zu realisieren. Nach ihrer Bewährung werden die neuen Datenschutzkonzepte des TDDSG nun für den allgemeinen Datenschutz in das Bundesdatenschutzgesetz übernommen werden. Die Grundsätze zur Datenvermeidung und -sparsamkeit, zum Systemdatenschutz, zur Anonymität und Pseudonymität werden dann als übergreifende Prinzipen für das gesamte Datenschutzrecht gelten. Um aber wirklich guten Datenschutz zu gewährleisten, genügen gute Gesetze allein nicht. Es wird darauf ankommen, sie auch adäquat umzusetzen.