erschien in: H. Bäumler, A. von Mutius (Hrsg.): Datenschutzgesetze der dritten Generation, Texte und Materialien zur Modernisierung des Datenschutzrechts; Luchterhand, Neuwied 1999, 18-27

Datenschutz durch Technik

Andreas Pfitzmann
Fakultät Informatik, TU Dresden
D-01062 Dresden
pfitza@inf.tu-dresden.de

Eine Ordnung des Gebietes „Datenschutz durch Technik“ wird entwickelt, in die die bekannten Datenschutzmaßnahmen einsortiert werden. Dies erleichtert Überblick und Verständnis.

1 Motivation

Wirksamer Datenschutz benötigt nicht nur rechtliche Grundlagen und organisatorische Maßnahmen, sondern auch technische. Anders gesagt: Bereits die Technikgestaltung muß sich am Ziel Datenschutz orientieren. Datenschutz durch Technik wird oft auch *Systemdatenschutz* genannt.

Das Gebiet „Datenschutz durch Technik“, ein Teilgebiet der Informatik, hat in den knapp 2 Jahrzehnten seines Bestehens einen stürmischen Aufschwung genommen. Es ist folglich lohnend, für die entwickelten Datenschutzmaßnahmen eine Ordnung zu finden. Sie kann einerseits helfen, die Übersicht zu behalten oder wiederzugewinnen. Andererseits können die Ordnungskriterien vielleicht auch zur Bewertung von Datenschutzmaßnahmen dienen sowie ggf. zur Identifizierung von Lücken: Wo könnten vielleicht noch Datenschutzmaßnahmen erfunden und entwickelt werden? Welche Klassen von Datenschutzmaßnahmen werden in rechtlichen oder organisatorischen Regelungen nicht oder nur ungenügend beachtet?

2 Eine Ordnung der Datenschutzmaßnahmen

Für die Ordnung von Datenschutzmaßnahmen sind 2 Dimensionen hilfreich:

Dient die Maßnahme eher der **Vertraulichkeit** von personenbezogenen Daten oder dient die Maßnahme vor allem der **Korrektheit** personenbezogener Daten (inkl. ihrer Aktualität)?

Wie **stark** oder **schwach**, d.h. wie wirksam ist die Maßnahme in einem offenen System? In einem offenen System kann jeder teilnehmen, so daß in ihm Maßnahmen der Personalauswahl und -schulung sowie der rechtlichen Regelung allenfalls begrenzt greifen.

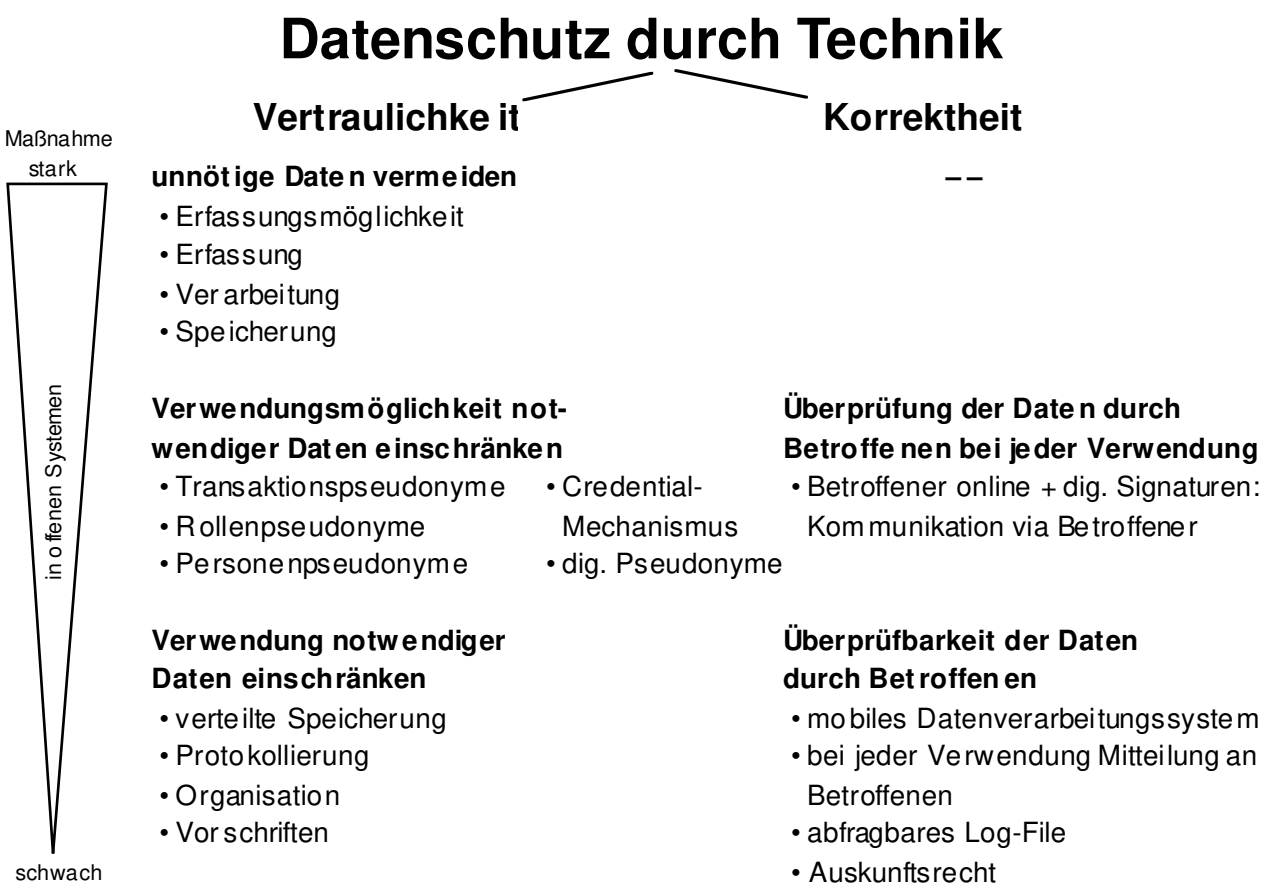
Die folgende Tabelle nutzt diese 2 Dimensionen zur Ordnung der bekannten Datenschutzmaßnahmen, wobei ich Maßnahmen mit gleichem Ziel und ähnlicher Wirksamkeit mittels Überschriften gruppiert habe.

Die Vertraulichkeit von Daten ist dann am stärksten, wenn sie vollständig vermieden werden können – was natürlich nur bei unnötigen 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 nötig, daß der einen Telekommunikationsdienst Erbringende erfährt, welche Kommunikationspartner er miteinander verbindet. In der Maßnahmengruppe **unnötige Daten vermeiden** (*Datenvermeidung*) lohnt es sich, zwischen Vermeiden der

- Erfassungsmöglichkeit, Schlagworte sind *Unbeobachtbarkeit, Anonymität, Unverkettbarkeit* [unbeobachtbare Kommunikation: Chau_81, Chau_88, Pfit_90, JMPP_98, Pfit_93, Fede_99; unbeobachtbare digitale Zahlungssysteme: Chau_85, Chau_89, Chau_92, BüPf_89, PWP_90], der
- Erfassung [unbeobachtete Kommunikation, unbeobachtete Geldtransaktionen, etc.], der
- Verarbeitung und der
- Speicherung

zu unterscheiden. Die letzten beiden Punkte gehören zum Bereich der *Anonymisierung*.

Um die Korrektheit von Daten, die es nicht gibt, braucht man sich keine Sorgen zu machen: Diese Maßnahmengruppe ist und bleibt leer.



Kann man Daten nicht vermeiden, so ist das Nächstbeste, die Verwendungsmöglichkeit notwendiger Daten einzuschränken bzw. die Daten bei jeder Verwendung durch den Betroffenen auf Richtigkeit und Aktualität überprüfen zu lassen. Das Ziel der *Datensparsamkeit* umfaßt, die Verwendungsmöglichkeit notwendiger Daten einzuschränken.

Bei Betonung der informationellen Aspekte, d.h. welche Informationen worüber sind verfügbar, kann man konkretisierend von *informationeller Zweckbindung* sprechen, bei Betonung der Umsetzung durch technische Komponenten von *Zweckbindung durch Technik*.

Das wesentliche Hilfsmittel, die **Verwendungsmöglichkeit notwendiger Daten einzuschränken**, ist die Verwendung von Pseudonymen anstelle der üblichen Personenidentitäten [PWP_90].

- Transaktionspseudonyme sind am wirksamsten, da sie jeweils nur für einen einzigen Vorgang verwendet werden, also keinerlei Verkettung von verschiedenen Vorgängen ermöglichen.

- Rollenpseudonyme dienen zur Verkettung der Vorgänge innerhalb einer Geschäftsbeziehung, werden allerdings für jede Geschäftsbeziehung unterschiedlich gewählt.
- Personenpseudonyme sind Personen zugeordnet und werden von ihnen in unterschiedlichen Rollen für die unterschiedlichsten Geschäftsbeziehungen und Transaktionen verwendet. Hierdurch ermöglichen Personenpseudonyme die Verkettung aller dieser Vorgänge und damit in der Regel bereits nach kurzer Zeit eine (Re-)Identifizierung des Pseudonymträgers.

Es sei hervorgehoben, daß zur Gewährleistung von Rechtssicherheit und Schadensvermeidung keineswegs eine Aufdeckbarkeit der Pseudonyme durch Dritte nötig ist, wie sie beispielsweise im Signaturgesetz gefordert und im gesamten Informations- und Kommunikationsdienste-Gesetz unterstellt ist. Sicherer Werteaustausch ist mittels geeigneter Protokolle auch ohne diese Aufdeckmöglichkeit möglich [BüPf_90, PWP_90]. Pseudonyme, die von Dritten nicht aufgedeckt werden können, bieten zweifellos stärkere Vertraulichkeit. Durch Dritte aufdeckbare Pseudonyme sind ein Beispiel für verteilte Speicherung und werden weiter unten eingeordnet.

Die stärkste Maßnahme, die Korrektheit von Daten sicherzustellen, ist die **Überprüfung der Daten durch den Betroffenen bei jeder Verwendung**. Ohne elektronische Vernetzung von BürgerInnen, Verwaltungen und Firmen ist dies für viele Anwendungen zu aufwendig. Sobald der Betroffene online ist und die Unverfälschtheit von Daten mittels digitaler Signaturen gesichert werden kann, kann alle Kommunikation von personenbezogenen Daten über den Betroffenen erfolgen, so daß er Richtigkeit, Aktualität, Relevanz und Vollständigkeit seiner Daten überprüfen kann. Dies bedeutet nicht notwendigerweise, daß er immer als Mensch involviert ist, sondern er kann Routinevorgänge auch nach seinem Dafürhalten an seinen persönlichen Rechner delegieren. Der bereits heute gültige Grundsatz der Erhebung personenbezogener Daten vorzugsweise beim Betroffenen ist ein Spezialfall der gerade beschriebenen Maßnahme.

Hochinteressant ist, daß die Einschränkung der Verwendungsmöglichkeiten von Daten und die Überprüfung der Daten durch den Betroffenen bei jeder Verwendung trefflich **kombiniert** werden können:

- Im einfachsten Fall erlauben dies digitale Pseudonyme, die nichts anderes sind als Testschlüssel digitaler Signatursysteme, wie sie beispielsweise mittels PGP vollkommen anonym erzeugt und bei Bedarf mehr oder weniger anonym zertifiziert werden können.
- Besteht die Notwendigkeit, digital signierte Dokumente, die auf ein Transaktions- oder Rollenpseudonym ausgestellt sind, auf ein anderes Transaktions- oder Rollenpseudonym derselben natürlichen Person umzuformen, sind aufwendigere Verfahren nötig, über die als erster David Chaum publiziert hat [Chau_85, Chau_87, Chau_90].

Diese aufwendigeren Verfahren sind natürlich viel datenschutzfreundlicher als der naive Ansatz, dem Empfänger des signierten Dokuments mitzuteilen oder gar zu beweisen, daß beide Pseudonyme derselben natürlichen Person gehören. Denn wer wollte den Empfänger dieser Information hindern, sie auch in anderem Kontext zu verwenden?

Soweit die starken Maßnahmen. Für Vermeiden der Erfassungsmöglichkeit unnötiger Daten durch Unbeobachtbarkeit, Anonymität und Unverkettbarkeit sowie Zweckbindung durch Verwendung teilnehmergewählter Pseudonyme hört man heutzutage den schönen Namen *Selbstdatenschutz*. Mittels geeigneter kryptographischer Verfahren, eingebettet in persönliche Rechner und gestaltbar mittels auch von Laien bedienbarer Oberflächen kann sich jede(r) weitgehend selbst schützen.

Die schwächsten dargestellten Maßnahmengruppen schränken die Verwendung notwendiger Daten ein bzw. stellen Überprüfbarkeit durch den Betroffenen her. Sie sind nicht notwendigerweise das Schlechteste: Gar nichts tun ist sicherlich schlimmer und selbst Überprüfbarkeit durch Stellvertreter (z.B. Datenschutzbeauftragte) ist schwächer.

Die **Verwendung notwendiger Daten einschränken** (*Zweckbindung durch Organisation und Recht*) können

- verteilte Speicherung, d.h. mehrere speichernde Stellen müssen kooperieren, damit die jeweils vorliegenden Teile der Daten genutzt werden können (bei Verwendung von *Kryptographie* beispielsweise müssen Schlüsseltext und Schlüssel zusammengeführt werden, um zu Entschlüsseln; oder nach einer *Pseudonymisierung* müssen die Stelle, die die pseudonymisierten Daten speichert, sowie die Stelle, die die Identifizierungsinformation zu den Pseudonymen verwaltet, zusammenarbeiten, um die Daten wieder personenbezogen verarbeiten zu können),
- Protokollierung, d.h. es ist hinterher technisch feststellbar, wer welche Daten wozu genutzt hat,
- Organisation, d.h. Arbeitsorganisation inkl. Kontrolle, sowie
- Vorschriften, d.h. Verfassung, Gesetze, Verordnungen und Vereinbarungen.

Überprüfbarkeit der Daten durch Betroffene herstellen bzw. unterstützen können

- mobile Datenverarbeitungssysteme, d.h. die personenbezogenen Daten befinden sich auf Datenträgern im Besitz des Betroffenen, z.B. auf Chipkarten,
- Mitteilungen an den Betroffenen bei jeder Verwendung von Daten (auch dies ist nur dann generell praktizierbar, wenn der Betroffene online ist),
- durch den Betroffenen via Netz abfragbares oder vor Ort einsehbares Log-File (nur ersteres dürfte wirksam sein, wobei die Abfrage selbstverständlich auf Einträge zu begrenzen ist, die den Betroffenen betreffen), und – last and least – natürlich das ganz konventionelle
- Auskunftsrecht, das vielleicht via Netz häufiger in Anspruch genommen wird.

3 Diskussion der Ordnung

Die Sortierung nach stark bzw. schwach in offenen Systemen sagt naturgemäß wenig darüber aus, wie stark bzw. schwach die Maßnahme in einem geschlossenen, d.h. abgeschotteten, System ist. Beispielsweise können organisatorische Maßnahmen hochwirksam sein in Umgebungen, wo Telekommunikation die Ausnahme ist, da die Rechner nicht vernetzt sind und mobile Datenträger (z.B. Disketten) kontrolliert werden. Allerdings dürfte dies, was vor 10 Jahren noch die Regel war, bereits heute, spätestens jedoch in 10 Jahren eine exotische Ausnahme sein.

Die von mir favorisierten starken Maßnahmen der Datenvermeidung und Einschränkung der Datenverwendungsmöglichkeit erfordern, daß spätestens mit dem Betrieb des Systems dessen Ziele abschließend klar sind. Dies sollte eigentlich für datenschutzrelevante Systeme eine Trivialität sein, dürfte aber in der Praxis wohl eher nicht der Fall sein. Dort mag durchaus das Bedürfnis bestehen (ob ihm nachgegeben werden sollte, ist eine andere Frage), erst einmal Daten zu sammeln, um dann später (ex post) zu entscheiden, ob und ggf. wie sie genutzt werden. Starke Maßnahmen sind in diesem Sinne *starr* (Entscheidung ex ante), schwache Maßnahmen *flexibel*.

Vielleicht noch eine einschränkende Bemerkung zur stärksten (und starrsten) Maßnahme: Ob die Erfassungsmöglichkeit unnötiger Daten vermieden wird, hängt u.a. von der Systemdefinition ab. Beispielsweise kann, etwa in ungewöhnlichen Situationen, auch eine Erfassung im Umfeld des Systems erfolgen. So ist etwa eine konventionelle Strafverfolgung selbst bei Anwendung dieser stärksten Maßnahme im informationstechnischen System weiterhin möglich. Ein Beispiel ist die akustische Überwachung von Räumen, z.B. im Rahmen des sogenannten Großen Lauschangriffs. Damit können u.a. Telefongespräche unabhängig davon überwacht werden, wie sie innerhalb des Telekommunikationssystems geschützt werden.

Die Stärke bzw. Schwäche von Maßnahmen hängt davon ab, *gegen wen* ihre Wirkung betrachtet wird, d.h. sie ist vom zugrundegelegten Angreifermodell abhängig. Bisher habe ich als Angreifer die Beteiligten, beispielsweise die Kommunikationspartner, unterstellt und Alternativen, etwa die Betrachtung Unbeteiligter, beispielsweise von Personen, die die Kommunikation abhören, nicht diskutiert. Hier sei nur angedeutet, daß diese Betrachtung unterschiedlicher Angreifer nötig ist und zu einer Erweiterung der Ordnung der Datenschutzmaßnahmen führt: Statt einer Dimension für die Stärke bzw. Schwäche von Maßnahmen ist im schlimmsten Fall für jeden betrachteten Angreifer eine eigene Dimension nötig. Das allgemein Gesagte sei am Beispiel Verschlüsselung erläutert: Zunächst wird Verschlüsselung als Schutzmaßnahme vor *Beteiligten* betrachtet. Dann kann es nur um den Schutz zu speichernder Daten gehen, wie oben erläutert wurde, und die Maßnahme ist unter „Verwendung notwendiger Daten einschränken; • verteilte Speicherung“ einzuordnen. Wird Verschlüsselung jedoch als Maßnahme gegen *Unbeteiligte* angewendet, dann vermeidet sie, daß die Unbeteiligten die Nachrichteninhalte überhaupt erfassen können. Verschlüsselung ist dann unter „unnötige Daten vermeiden; • Erfassungsmöglichkeit“ einzuordnen.

4 Ausblick

Die hier vorgeschlagene Ordnung, so hilfreich sie schon im jetzigen Zustand ist, muß je nach Verwendungszweck verfeinert und durch Diskussionen validiert werden – ich freue mich über Kommentare jeder Art. Sicherlich können innerhalb der einzelnen Maßnahmengruppen weitere Beispielmaßnahmen gefunden, vielleicht sogar im Laufe der Zeit neue Maßnahmengruppen identifiziert werden. Die Literaturliste ist bei weitem nicht vollständig, ich habe versucht, in den Verfahrensklassen zumindest die frühesten Papiere zu zitieren. Die Zahl der Folgepapiere geht ins Uferlose. Trotzdem ist es zumindest für die Forschung sinnvoll, eine ggf. verfeinerte Ordnung mit vollständiger Literaturliste zu erstellen und zu pflegen.

5 Bedeutung der Ordnung für das LDSG-neu

Die oben entwickelte Ordnung kann benutzt werden, um zu prüfen, inwieweit der Entwurf des LDSG-neu [Schleswig-Holsteinischer Landtag, Drucksache 14/1738] das Gebiet datenschutzfreundlicher Technologien abdeckt.

Gut vertreten im Entwurf des LDSG-neu sind die Sachverhalte *Systemdatenschutz*, *Datenvermeidung*, *Anonymisierung*, *Zweckbindung durch Organisation und Recht*, *Kryptographie*, *Pseudonymisierung*, *Protokollierung*, *Organisation*, *Vorschriften*, *mobile Datenverarbeitungssysteme* und *Auskunftsrecht*. Auch das Konzept *Selbstdatenschutz* ist vorhanden.

Nicht vorhanden im Entwurf des LDSG-neu sind bisher die drei Maßnahmengruppen zu *Zweckbindung durch Technik*. Hier wäre eine Ergänzung des Entwurfs des LDSG-neu wünschenswert. Aufgenommen werden sollten Pseudonyme, die Benutzer selbst wählen und die durch Dritte nicht aufdeckbar sind sowie, ggf. kombiniert, Maßnahmen zur Überprüfung der Daten durch den Betroffenen bei jeder Verwendung.

6 Weitere Anmerkungen zum Entwurf für ein LDSG-neu

Den „10 Geboten“ zur Datensicherheit gebührt ein würdiger Platz in der Rechtsgeschichte. Für moderne Datenverarbeitung in offenen Netzen sind sie weitgehend irrelevant. Deshalb begrüße ich, daß der Entwurf des LDSG-neu auf sie verzichtet.

Ich begrüße eine Konzentration auf das Wesentliche, habe aber Zweifel, ob personenbezogene (oder auch nur personenbeziehbare) Daten nach Sensibilität gestuft werden können und sollten. Aus vielen einzeln völlig harmlosen Daten lassen sich sehr sensitive Daten gewinnen. Kurzum: Ich halte die Schalentheorie aus Sicht der Informatik nicht für zutreffend.

Ich hätte erwartet, daß Datenverarbeitung auch einen Datenverarbeitungsschritt enthält, den wir Informatiker mit *processing* bezeichnen würden.

Aus meiner Sicht bezieht sich der Begriff „Audit“ auf Prozesse und nicht auf Produkte. Ich würde also die Begründung zu §4 leicht ändern.

§24 „Besondere Dokumentationsstelle für Sekten“ gehört nicht ins LDSG. Wenn dies gesetzlich geregelt werden muß, dann bitte in einem eigenständigen Gesetz. Datenschutz ist keine Weltanschauung und sollte nicht durch einen Paragraphen, der den Umgang mit verqueren Weltanschauungen regelt, in diesen Kontext gestellt werden.

7 Literatur

BüPf_89 Holger Bürk, Andreas Pfitzmann: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399-416.

BüPf_90 Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

Chau_85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

Chau_87 David Chaum: Sicherheit ohne Identifizierung; Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen; Informatik-Spektrum 10/5 (1987) 262-277; Datenschutz und Datensicherung DuD 12/1 (1988) 26-41.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988) 65-75.

Chau_89 David Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards, Proceedings of the IFIP WG 11.6 International Conference; Laxenburg (Austria), 19.-20. 10. 1987, North-Holland, Amsterdam 1989, 69-93.

Chau_90 David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt '90, Sydney, Australia, January 1990, LNCS 453, Springer-Verlag, Berlin 1990, 246-264.

Chau_92 David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.

Fede_99 Hannes Federrath: Sicherheit mobiler Kommunikation; DuD-Fachbeiträge, Vieweg, Wiesbaden 1999.

JMPP_98 Anja Jerichow, Jan Müller, Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol; IEEE Journal on Selected Areas in Communications 16/4 (1998) 495-509.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; IFB 234, Springer-Verlag, Berlin 1990.

Pfit_93 Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.