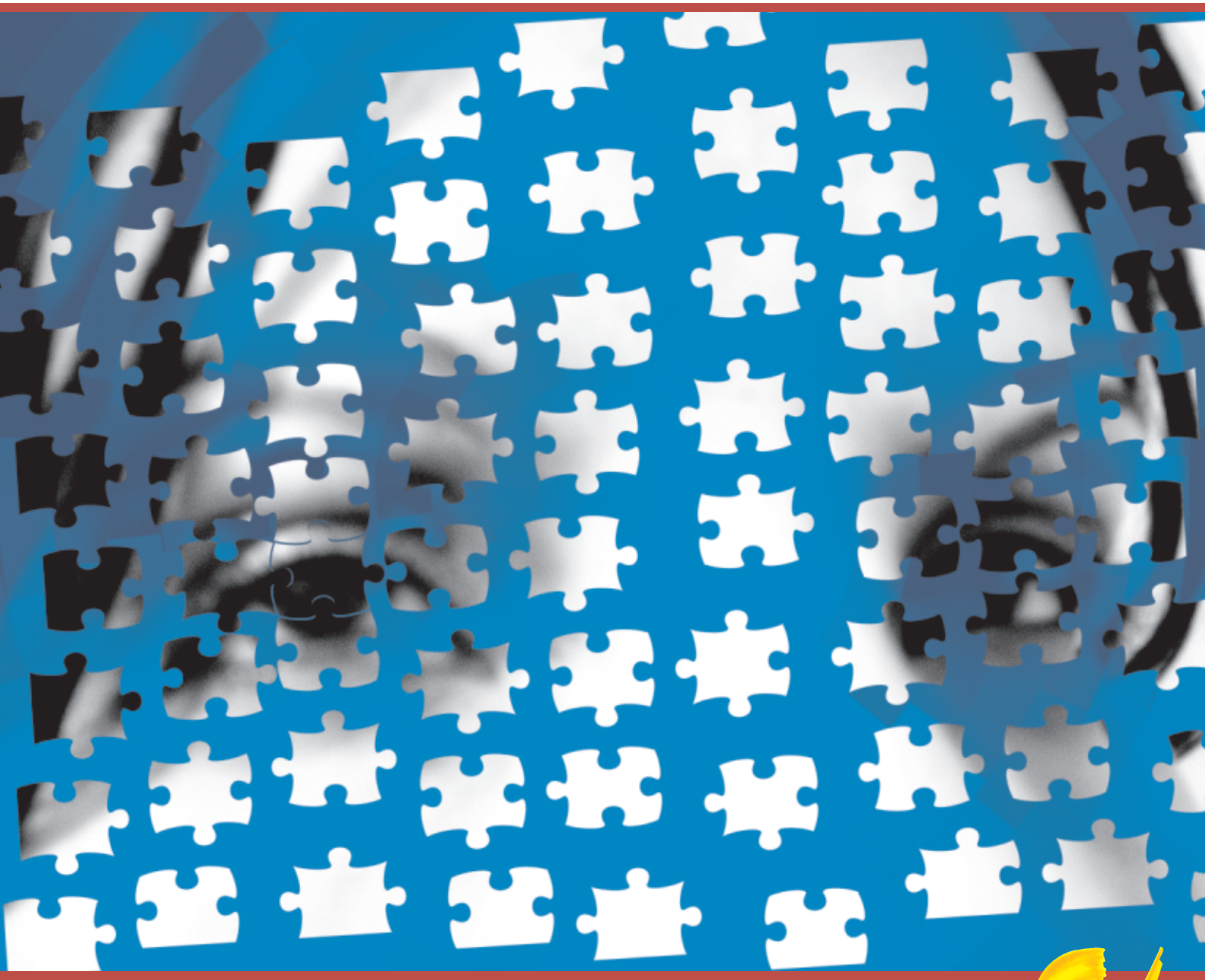
Verkettung digitaler Identitäten



TECHNISCHE UNIVERSITÄT DRESDEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Verkettung digitaler Identitäten

Version 1.0

Projektnummer: PLI1563

Gefördert vom Bundesministerium
für Bildung und Forschung im Rahmen der
Innovations- und Technikanalyse

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Unterauftrag:
Technische Universität Dresden
Professur Datenschutz und Datensicherheit

Beiträge zu diesem Report:

Unabhängiges Landeszentrum
für Datenschutz Schleswig Holstein (ULD)
Holstenstr. 98, 24103 Kiel
Tel.: +49 431/988-1200, Fax: +49 431/988-1223
mail@datenschutzzentrum.de, https://www.datenschutzzentrum.de/

Marit Hansen (Editor)
Sebastian Meissner (Editor)

Beiträge von:
Marit Hansen
Markus Hansen
Marita Häuser
Kai Janneck
Henry Krasemann
Martin Meints
Sebastian Meissner
Maren Raguse
Martin Rost
Jan Schallaböck

Technische Universität Dresden
Professur Datenschutz und Datensicherheit
Nöthnitzer Str. 46, 01187 Dresden
Tel.: +49 351/463-38247, Fax: +49 351/463-38255
pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Beiträge von:
Sebastian Clauß
Sandra Steinbrecher
Andreas Pfitzmann

Kiel, Oktober 2007

Umschlaggestaltung: Markus Hansen
ISBN: 9783000234064

Danksagung

Der Dank des Autoren-Teams für die Unterstützung beim Vorhaben „Verkettung digitaler Identitäten“ geht an Christian Krause für die Erstellung der Graphiken sowie an Nils Bergemann, Meike Kamp, Ulrich Stockter und Dr. Thilo Weichert vom ULD für eine intensive Diskussion und viele wertvolle Beiträge.

Weiterhin geht ein Dankeschön an die Organisatoren der vier Workshops in Kiel und Dresden sowie alle Helfer, die zu einem reibungslosen Ablauf und einer angenehmen Arbeitsatmosphäre beigetragen haben.

Gedankt sei auch denen, die über die letzten Monate – eigentlich sogar Jahre – in intensivem Brainstorming, mit Impulsvorträgen und teils hitziger Debatte das Thema geformt und die Ergebnisse frei gelegt haben.

Schließlich danken wir den Entwicklern der freien Textverarbeitung OpenOffice, die eine plattformübergreifende Zusammenarbeit mit stabiler Open-Source-Software möglich gemacht haben.

Verkettung digitaler Identitäten
– Executive Summary –

Das gesamte gesellschaftliche Leben basiert auf ***Verkettung***, also der Verbindung von Entitäten wie Subjekten und Objekten miteinander. Namen, die Personen zugeordnet werden, wie auch Bezeichner von Objekten bilden ein Bindeglied zwischen einer Zeichenkette und dem bezeichneten Subjekt bzw. Objekt. Mehrere Daten zu einem Subjekt (oder Objekt) lassen sich verketten und dadurch angereicherte Information liefern. Die Arbeit befasst sich mit tatsächlichen ***Verkettungen***, ***Verkettbarkeit*** (d.h. der Möglichkeit von Verkettung) und der ***Unverkettbarkeit*** (d.h. der Unmöglichkeit von Verkettung) in verschiedenen Facetten. Außerdem erörtert sie das Konzept des ***Entkettens*** zur Abtrennung von Einzeldaten aus bereits verketteten Informationen.

Weil Menschen miteinander verbunden sind, gibt es die ***Gesellschaft***. Die Gesellschaft hat Bestand, weil sie nicht nur in einem einzelnen Augenblick existiert, sondern weil sie Verbindungen zur Vergangenheit hat sowie Pläne oder zumindest Optionen für die Zukunft. Die Gesellschaft bezieht ihre relative Stabilität auch deshalb, weil sie in ihrer Vergangenheit verwurzelt ist. Aus ihrer Geschichte kann eine Gesellschaft lernen und ihre Traditionen pflegen, entwickeln und weitergeben.

Organisationen – unabhängig davon, ob es sich um öffentliche Verwaltungen, Unternehmen oder Vereine handelt – sind typischerweise „Verkettungsmaschinen“. Mit dem Ziel, Entscheidungen vorzubereiten und zu treffen, verketten sie vielfältige Entitäten für ihre jeweiligen Zwecke.

Dasselbe gilt für jedes ***Individuum*** in der Gesellschaft. Jeder hat normalerweise ein intuitives Verständnis von Verkettungen und Verkettbarkeiten. Dieses Verständnis ist wesentlich, um die eigene Position in der Gesellschaft zu finden und mit anderen sozial zu interagieren. Genauer ausgedrückt basiert die individuelle Selbstbestimmung – ein Konzept von besonderer Relevanz für den Datenschutz – auf

1. der ***Transparenz*** von möglichen und tatsächlichen Verkettungen und ihrem Grad an (Un-) Verkettbarkeit sowie
2. der Möglichkeit des Individuums, Verkettung und Unverkettbarkeit zu ***steuern*** – zumindest in gewissem Umfang, wobei dieser ebenfalls für das Individuum transparent sein muss.

In der digitalen Welt spielt das Grundkonzept von Verkettung und (Un-)Verkettbarkeit sogar eine noch wichtigere Rolle, insbesondere wenn es um Datenverarbeitung in globalen Netzen geht. Jede Person hat eine wachsende Zahl von Identifikatoren und ihnen zugeordnete Identitätsattribute, z.B. in der Eigenschaft als Staatsbürger, als Kunde einer bestimmten Firma, als Angerufener oder als Nutzer einer Auktionsplattform im Internet. ***Digitale Identitäten***, die eine Person in der digitalen Welt repräsentieren, sind oft verkettet mit Informationen über diese Person, wie etwa ihre sozialen Kontakte oder bestimmte Handlungen, die sie unter Nutzung dieser digitalen Identität vorgenommen hat. Diese Informationen können verfeinert oder erweitert werden, indem sie mit anderen Datenquellen, z.B. anderen digitalen Identitäten derselben Person, verkettet werden oder indem Scoring-Verfahren oder andere ausgeklügelte Algorithmen eingesetzt werden, um die Informationen auszuwerten.

Ein paar Beispiele verdeutlichen die für die Verkettung relevanten Aktivitäten in verschiedenen Bereichen: Reputationssysteme basieren darauf, Daten von früheren Interaktionen einer Person zu verketten, um ihr zukünftiges Verhalten vorherzusagen. Data-Mining-Systeme werden benutzt, um jene Menschen herauszufiltern, die mit der höchsten Wahrscheinlichkeit ein bestimmtes Produkt kaufen, wobei alle verfügbaren Informationen verkettet und mit komplexen Algorithmen analysiert werden. Ähnlich geht die Polizei vor, wenn sie Straftäter aus der Masse der rechtstreuen Bürger herausfinden will. Auf der anderen Seite nutzen selbstverständlich auch die Straftäter Verkettungstechniken, um „lohnende“ Opfer ausfindig zu machen.

Wie sehr Verkettung, Verkettbarkeit und Unverkettbarkeit in einer bestimmten Situation gewünscht ist, kommt auf den Kontext und auf die Perspektive der beteiligten Parteien an. Um die Eigenschaften und Potenziale von Verkettungen zu verstehen, muss deutlich herausgearbeitet werden, wer auf welche Daten zugreifen kann und was mit ihnen geschieht. Von einzelnen Szenarien abstrahierend, identifiziert diese Arbeit die folgenden wichtige Rollen und Teilaufgaben im ***Workflow der Informationsanreicherung*** durch Verkettung:

- den ***Adress-Provider,*** der einer Person Identifikatoren oder Adressen gemäß einem definierten Adressschema zuordnet, das von einem ***Adressschema-Provider*** zur Verfügung gestellt wird;
- den ***Datensammler,*** der die Informationen beobachtet und speichert;
- den ***Verketter,*** der die gesammelten Daten verbindet, indem er Verkettungsalgorithmen nutzt, die u.U. von einer dritten Seite bereitgestellt werden können, dem ***Verkettungsalgorithmus-Provider;***
- den ***Auswerter,*** der die Daten unter Nutzung von Algorithmen (so genannten Modellen) analysiert, die wiederum u.U. von einer weiteren Partei bereitgestellt werden können, dem ***Auswertungsalgorithmus-Provider*** (oder ***Modell-Provider***);
- den ***Entscheider,*** der auf Grundlage der verfügbaren Informationen eine Entscheidung fällt;
- den ***Betroffenen,*** der betroffen ist von der gefällten Entscheidung und ihren Konsequenzen.

In sämtlichen identifizierten Teilschritten des Prozesses tragen die Akteure in irgendeiner Form zur Verkettbarkeit bei und müssen daher umsichtig vorgehen, um unerwünschte Effekte zu vermeiden. Taucht nämlich ein Fehler auf, kann es für den Betroffenen ausgesprochen schwierig sein, diesen Fehler und seine Ursache im Prozess zu finden und eine angemessene Korrektur der Maßnahme herbeizuführen.

Im Normalfall ist Verkettung – und auch schon die Verkettbarkeit – unzweifelhaft datenschutzrelevant, da das Recht auf informationelle Selbstbestimmung („wer weiß was über mich“) berührt ist. Allerdings ist nicht in allen Fällen das Datenschutzrecht anwendbar, weil die Verbindung zu einer bestimmten natürlichen Person nicht mit hinreichender Sicherheit hergestellt werden kann. So können auch anonyme Profile Informationen enthalten, die eine Diskriminierung von Individuen ermöglichen, oder der Personenbezug kann später hergestellt werden, z.B. mittels zusätzlicher Verkettungsalgorithmen, gestiegener Rechenleistung oder ergänzender Daten. Insoweit ***geht das Konzept der Verkettung und Verkettbarkeit über die europäische Datenschutzgesetzgebung hinaus***.

Das zentrale Ziel dieser Arbeit ist es, die ***Bedingungen an Verkettung, Verkettbarkeit und Unverkettbarkeit*** – besonders in der digitalen Welt – zu untersuchen und zu zeigen, welche Effekte organisatorische und technische Maßnahmen in diesem Bereich zeitigen können. Hervorgehoben sei hier das Konzept der ***pseudonymen Beglaubigungssysteme*** (engl.: „pseudonymous convertible credentials“), denn es kombiniert Zurechenbarkeit und Anonymität, indem es dem Nutzer die Kontrolle über den Zuschnitt seiner Verkettbarkeiten nach vordefinierten Regeln (z.B. durch die Gesellschaft) überlässt. Diese Credential-Technologie birgt das Potential, die Gesellschaft zu verändern. Denn es garantiert faires Nutzerverhalten – oder legt dies zumindest nahe, da unfaires Verhalten Sanktionen nach sich zieht –, indem die Privatsphäre der Akteure geschützt wird und gleichzeitig unerwünschte Effekte von Anonymität und Unverkettbarkeit vermieden werden.

Diese Arbeit untersucht den derzeitigen ***Stand der Verkettung*** in drei zentralen Kontexten:

1. ***Öffentliche Verwaltung:*** Hier werden im Wesentlichen sektorspezifische Informationen gesammelt, die teilweise über den Tod des Individuums hinaus gespeichert werden, beispielsweise weil sie für administrative Planungsprozesse benötigt werden. Der Betroffene hat in der Regel keine Möglichkeiten, die Datenmenge zu reduzieren oder die rechtlich definierten Verkettungsprozesse zu unterbinden. Die Daten werden nur selten für die Bildung psychologischer Profile verwendet. In Fällen der Strafverfolgung oder anderen ähnlichen Fällen hoheitlicher Gewaltausübung bekommen die Methoden einen stärker invasiven Charakter und bringen eine umfassendere Verkettung mit sich, wie etwa bei der Einführung der Vorratsdatenspeicherung.

2. ***Wirtschaft:*** Für die Wirtschaft ist es notwendig, Kunden für die angebotenen Dienstleistungen und Produkte zu interessieren. Die Anbahnung und Verstetigung von Kundenbeziehungen ist ein zentrales Ziel. Zu diesem Zweck versuchen viele Unternehmen, so viele Informationen wie möglich zu sammeln und zu verketten – jedenfalls solange sich dies insgesamt auszahlt. Ziel kann es sein, die geheimen Wünsche ihrer (potenziellen) Kunden zu erfahren oder aber ihre Bonität zu prüfen. Diese Datensammlung führt leicht zur Erstellung von aufschlussreichen Profilen zu Persönlichkeitsmerkmalen des Nutzers oder ähnlichen Informationen wie etwa dessen Interessen oder sein soziales Netzwerk. Auf Basis dieser Verkettungen können auch manipulative Techniken zum Einsatz kommen.
3. ***Communities:*** Der derzeitige Trend, freiwillig auch sensible Informationen zu veröffentlichen, ist besonders in Online-Communities zu erkennen. Während Verwaltung und Wirtschaft rechtlich eng im Umgang mit personenbezogenen Daten gebunden werden können – wie schwer das Durchsetzen der Rechtsnormen im Einzelfall auch sein mag – und sie ein gewisses Qualitätslevel einschließlich Authentizität von Daten oder Datensicherheitsmaßnahmen garantieren müssen, kann dies von Nutzern dieser Online-Communities nicht erwartet werden. Die Langzeitfolgen für die Individuen, deren Privatsphäre hier betroffen ist, aber auch für die Gesellschaft insgesamt, kann noch nicht abgeschätzt werden.

Diese Arbeit illustriert einige ihrer Ergebnisse anhand von vier ***Szenarien.*** Diese beleuchten jeweils spezifische Effekte, die sich bereits jetzt abzeichnen oder aber in baldiger Zukunft auftreten werden:

1. ***Überwachung mit Alltagsgegenständen:*** Viele Geräte und Apparate, die heute eingesetzt werden, erlauben die oftmals unbemerkte Überwachung anderer Personen, z.B. durch Tonüberwachung durch digitale Telefone, Videobilder durch Kamerahandys oder aber die Lokalisierung von Menschen anhand von RFID-Chips, die sie dicht am Körper tragen. Überdies kann sich jedermann preiswerte Spionagewerkzeuge (engl.: Spy Tools) über das Internet beschaffen.
2. ***Internet-Suchmaschinen:*** Die Benutzung des Internets umfasst üblicherweise auch die Verwendung von Suchmaschinen. Die eingegebenen Suchbegriffe offenbaren viele Informationen über den Nutzer, so z.B. über dessen aktuelle Interessen und Pläne. Dies gilt nicht nur für Einzelpersonen, sondern genauso für Unternehmen, deren Mitarbeiter möglicherweise unabsichtlich wichtige Geschäftsgeheimnisse durch die Eingabe verwandter Begriffe preisgeben, z.B. im Vorfeld von geplanten Fusionen und Übernahmen oder von Patenteintragungen. Üblicherweise speichern die Anbieter von Suchmaschinen ihren Datenbestand über sehr lange Zeiträume, oftmals auch außerhalb der Jurisdiktion des europäischen Datenschutzrechts. Die gespeicherten Daten können dann zu allen möglichen Zwecken verkettet werden.
3. ***Arbeitnehmerlokalisierung durch Location Based Services (LBS):*** Standortdaten stellen eine bedeutende Datenkategorie dar, da sie die räumliche Nachverfolgung (sog. Tracking) von Personen ermöglichen. In dem bezeichneten Szenario werden die technischen Möglichkeiten moderner LBS und der Wunsch eines Logistikunternehmens, zu wissen, wo sich seine Mitarbeiter aufhalten, der rechtlichen Verpflichtung zum Schutz der Privatsphäre der Arbeitnehmer gegenübergestellt.
4. ***„Ambient Assisted Living“:*** Eine sich abzeichnende Welt mit allgegenwärtigen Computern, in der jedes Objekt mit Sensoren ausgestattet ist, erlaubt eine schier grenzenlose Verkettung. Dies räumt auch neue Möglichkeiten für jene ein, die auf Hilfe beim Bestreiten des Alltags angewiesen sind, aber nicht in ein Pflegeheim ziehen wollen. Dienste des „Ambient Assisted Living“ können dazu beitragen, dieses Problem zu lösen, bergen aber gleichzeitig die Herausforderung, wie es gelingen kann, dabei die Privatsphäre und Würde der Menschen in einer Umgebung zu bewahren, in der alles verkettet werden kann.

Abschließend gibt diese Arbeit ***Handlungsempfehlungen für Entscheider*** in den Bereichen Technikgestaltung, Politik und Recht sowie Forschungsförderung. Die zentralen Empfehlungen adressieren insbesondere

- die Notwendigkeit von ***Transparenz*** und dem ***Verständnis der Nutzer*** in Bezug auf Verkettung und Verkettbarkeit,
- die Gestaltung von ***nutzergesteuertem Identitätsmanagement*** zur Befähigung der Nutzer, die Verkettung ihrer Daten zu kontrollieren,
- die Anforderung an ***Qualitätssicherung*** zur Vermeidung von unvorhersehbaren und fehlerhaften Resultaten und zum Vorsehen effektiver Möglichkeiten für die Korrektur aufgetretener Fehler sowie
- das Erfordernis von ***vertrauensbildenden Maßnahmen***, wie etwa einem IT-Grundschutz für die Computer der europäischen Bürger und die Schaffung von Angeboten, bei denen Nutzer nicht ihre Daten in Bereiche herausgeben müssen, in denen europäisches Datenschutzrecht nicht anwendbar oder nicht durchsetzbar ist.

Zusammengefasst ergibt sich, dass Verkettung und (Un-)Verkettbarkeit zentrale Konzepte für die ***Selbstbestimmung der Individuen in der heutigen demokratischen Gesellschaft*** darstellen. Dies gilt umso mehr, als die digitale Welt voller Identifikatoren für digitale Identitäten ist, die sich häufig ohne großen Aufwand verketten lassen. Um Gerechtigkeit in der Informationsgesellschaft zu bewahren und zu verbessern, müssen wir ***Verkettung und (Un-)Verkettbarkeit unter Bedingungen stellen***. Ein offener Diskussionsprozess sollte zu einem demokratischen Konsens über diese Bedingungen führen und auf ***technische Standards, Rechtsnormen sowie Best Practices für Datenverarbeiter*** einwirken.

Linking Digital Identities
– Executive Summary –

The whole life in society is based on ***linkage***, i.e., connecting entities like subjects and objects with each other. Names assigned to people as well as identifiers of objects are one evident link between a character string and the denominated subject or object. Data available on the same subject (or object) can be linked, yielding enriched information. The study deals with ***actual linkages***, ***linkability*** (i.e., possible linking) and ***unlinkability*** (i.e., impossibility of linking) in various flavors and discusses also the concept of ***de-linking*** to detach (partial) information from otherwise linked data.

Society itself only exists because people are connected to each other. Society subsists because it is not only alive in a single moment, but has ties to its past and plans – or at least options – for its future. Society is relatively stable because it is rooted in its past, having history to learn from as well as traditions to keep, to further develop and to pass on. ***Organizations*** – no matter whether they are public administrations, companies or associations – are typically linkage machineries which link various entities for their own purposes to prepare and render decisions.

The same is true for each ***individual*** in society. The individual usually has an intuitive understanding of links and linkabilities. This understanding is crucial for its positioning in society and for its basic need of social interaction. To be more exact, the individual's self-determination – a concept in particular relevant in the data protection area – bases on

1. ***transparency*** of possible and actual linkages as well as the degree of (un-)linkability as well as
2. the possibility for the individual to ***control*** linkage and (un-)linkability at least in a given range of options, which of course also have to be transparent to the individual.

In the digital world, the basic concept of linkage and (un-)linkability is even more important, in particular when it comes to data processing in global networks. Every person has a growing variety of identifiers and attached identity attributes, e.g., as being a citizen of a State, a customer of a company, a callee being called on a phone, or a user of an Internet auction service. ***Digital identities*** which represent people in the digital world are often linked with information about this very same person such as her social contacts or her actions performed under this digital identity. In addition, this information can be further specified or extended by linking it with other data sources, e.g., other digital identities of the same person, and utilizing scoring models or other sophisticated algorithms which analyze the data.

A few examples illustrate link-related activities in different settings: Reputation systems base on linking data from former interactions of a person to predict her future behavior. Data mining systems are used to find people who are most likely to buy certain products by linking and analyzing all information available using sophisticated algorithms. Similarly, police search systems try to detect offenders out of the mass of orderly citizens. Of course also offenders use linkage technologies to find out about worthwhile victims.

How much linkage, linkability or unlinkability is desired in a specific situation depends on its context as well as on the perspectives of the parties involved. For discussing linkage properties and objectives, it is important to make clearly visible who can access which data and perform which actions on these data. Generalizing from each specific setting, the study identifies important roles and tasks in the ***workflow of enriching data*** by linking them with other information:

- the ***address provider*** who assigns identifiers or addresses to a person according to an address schema defined by an ***address schema provider;***
- the ***data collector*** who monitors and stores information;

- the ***linker*** who connects collected data items according to linking algorithms, possibly being provided by another party, the ***linking algorithm provider;***
- the ***analyzer*** who analyzes the data by applying analysis algorithms (so-called models), possibly being provided by another party, the ***analysis algorithm provider*** (or ***model provider***);
- the ***decision maker*** who decides on basis of the information available at that stage;
- the ***data subject*** concerned by the decision and its consequences.

In all identified steps in the workflow, the actors contribute to some aspect of linkage and may have to be cautious to avoid undesired effects. In case of a mistake, it may be hard for data subjects to find the error and its cause in this workflow and to achieve that appropriate corrective measures are being taken.

Generally speaking, linkage as well as linkability is clearly privacy-relevant because it relates to the right of informational self-determination ("who knows what about me"). But not in all cases data protection law applies because, e.g., the link to a specific natural person cannot be established with a sufficient degree of certainty. Still even anonymous profiles can contain information which can be used to discriminate against individuals concerned, or the link to the individual can be established later, e.g., by additional linking algorithms, computing power or data. Insofar the control of linkability and linkage is an even ***wider concept than European data protection legislation***.

The main objective of this study is to discuss ***conditions for linkage, linkability and unlinkability*** – especially in the digital world – and to show which effects organizational and technical measures in this field may have. In particular the concept of ***pseudonymous convertible credentials*** should be highlighted here because it combines accountability and anonymity by putting the user in control to tailor linkability according to the predefined rules, e.g., given by society. This credential technology bears the potential of changing society as it guarantees – or, by imposing a sanction otherwise, at least strongly suggests – fair behavior of users by avoiding unwanted effects of anonymity and unlinkability while preserving privacy.

The study analyzes the ***status quo*** of linkage in three main contexts:

1. ***Public administration:*** Here mainly sector-specific information is collected and linked, partially longer than lifelong stored, e.g., needed for administrative planning processes. The data subject does not have possibilities to reduce the amount of data or prevent the legally defined linkage processes. The data rarely deal with psychological profiles. In cases of law enforcement and similar acts of sovereign power, the methods become more invasive and yield more linkage, such as the introduction of the data retention legislation.
2. ***Business:*** In the business sector it is relevant to get customers interested in the offered services and products. Establishing and maintaining customer relationships is a central objective. For this purpose, many companies try to collect and link as many data as possible – as long as it pays off – to, e.g., find out the secret desires of customers(-to-be) and check out their creditworthiness. Often this data collection leads to processing informative profiles on the user's personality traits or related characteristics such as interests or information about the user's social network. Manipulative techniques can build upon these data linkages.
3. ***Communities:*** The upcoming trend of people voluntarily disclosing also possibly sensitive information to others can be seen in particular in online communities. Whereas the public service and business sector are bound to law – however difficult to enforce – and have to guarantee a defined level of quality including authenticity of data or security safeguards, this cannot be expected from peers users meet in online communities. The long-term consequences for individuals whose privacy is at stake and for society as a whole are yet to be determined.

The study illustrates some of its findings in four ***scenarios*** which illuminate specific aspects relevant already today or in the foreseeable future:

1. ***Everyday's surveillance technology:*** Many devices and equipment used in everyday life allow for often unnoticed surveillance of others, e.g., by audio observation by digital telephone systems, in addition video observation by mobile camera phones, or tracking people by reading out RFID chips near their body. Mostly inexpensive spy tools are available for everybody, e.g., ordered via the Internet.
2. ***Internet search engines:*** Using the Internet usually involves search engines. The entered search terms reveal much information on the user, e.g., what she is interested in right now, what she is planning etc. This is not only true for individuals, but also for organizations whose employees unintentionally may disclose important business secrets by entering related words in search engines, e.g., ahead of a planned merger or acquisition of companies, or of taking out a patent. Usually providers of search engines store these data for a very long time outside the effective jurisdiction of European data protection law. The data stored there are possibly being linked for arbitrary purposes.
3. ***Employee tracking by location-based services (LBS):*** Location data is an important data category which may enable tracking. In this scenario technological possibilities of modern LBS and the desire of a logistics company to know the location of their employees are contrasted with the legal obligation to protect the employees' privacy.
4. ***Ambient Assisted Living:*** The future world of ubiquitous computing where every object maybe equipped with sensors allows for sheer unlimited linkages. This offers options for people who need some support in living, but who don't want to move to a nursing home. Services of Ambient Assisted Living can contribute to solve this problem, but bear the challenge how to preserve the people's privacy and dignity in a setting where everything can be linked.

The results of the study give ***guidance to decision makers*** in technology development, in politics and law, and in research promotion. The main recommendations address in particular

- the necessity of ***transparency*** and the ***users' understanding*** on linkage and linkability,
- the design of ***user-controlled identity management*** to empower users to control linkage of their personal data,
- the requirement for ***quality assurance*** in order to avoid uncertainties providing unpredictable and erroneous results as well as to provide effective possibilities for correcting occurred errors, and
- the need for ***trust-building measures***, such as measures to guarantee (at least) minimal level of data security for European citizens' computers and offering them services without having to disclose their data to areas where European law does not apply and would not be enforceable.

Summarizing, linkage and (un-)linkability are important concepts for ***self-determination of individuals and today's democratic society***. This is even more true in the digital world full of identifiers for digital identities which often can easily be linked. To maintain and enhance fairness in the information society, we have to ***consider conditions for linkage and (un-)linkability***. An open discussion process should lead to a democratic consensus about those conditions and ***influence technical standards, legal regulations as well as best practices for data processing entities***.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Diese Arbeit beschäftigt sich mit Verkettung digitaler Identitäten: „Verketten“ wird im weitesten Sinne aufgefasst, d.h., es geht nicht nur um das Zusammenführen von personenbezogenen Daten zur Erstellung eines Personenprofils, sondern ausgehend vom Konzept der Bezeichner und Adressen gehören zum Inhalt dieser Arbeit ebenfalls die Prozesse „Daten sammeln“, „Verknüpfen (bzw. Verketten im engeren Sinne)“, „Auswerten“ und „Generieren von Entscheidungen“, die Folgen für einen oder mehrere Betroffene[1] haben. Auch „digitale Identitäten“ werden im weiten Sinne verstanden, d.h. als jede mögliche Form von technisch abgebildeten Daten, die zu einer Person gehören. Dies bedeutet nicht automatisch, dass für einen Dritten ein eindeutiger Personenbezug dieser Daten gegeben ist. Daneben schränkt die Ausrichtung auf digitale Identitäten diese Arbeit nicht auf die digitale Online-Welt ein, denn zum einen sind verschriftlichte (Offline-)Daten Teile von digitalen Identitäten, und zum anderen ergibt sich häufig spätestens bei den getroffenen Entscheidungen und Folgen für Betroffene üblicherweise einen Bezug zur „realen“ Welt.

Während das Konzept der Verkettung (oder vielmehr der Unverkettbarkeit) seit Jahren schon in der technischen IT-Sicherheitsszene etabliert ist, spricht man im juristischen Bereich eher von Verknüpfungen. Auch die Begriffe Zusammenführen oder Vernetzen beschreiben, dass Entitäten wie Subjekte und Objekte in Beziehung gesetzt werden. Daneben finden sich verwandte Termini wie Typisierung, Profiling, Kategorisierung oder Klassifizierung, die ebenfalls Aspekte liefern, die in dieser Arbeit untersucht werden. Die weite Auffassung des Themas „Verkettung digitaler Identitäten“ ermöglicht die Diskussion von vielerlei Facetten und Stellschrauben, die die Auswirkungen auf Individuen, Organisationen und die Gesellschaft als Ganzes beeinflussen.

Abschnitt 1.1 gibt zunächst einen Überblick, bei welchen Gelegenheiten (fast) jedermann Datenspuren hinterlässt, die sich dann auch zur Verkettung eignen und interessante Aussagen zur Person liefern können. Dass es nicht um „gute“ oder „schlechte“ Verkettung geht, zeigt Abschnitt 1.2 auf, in dem argumentiert wird, dass stattdessen „erwünscht“ und „unerwünscht“ aus der unterschiedlichen Perspektive der jeweils Beteiligten die relevanten Eigenschaften sind.

Nach der Einleitung werden in Kapitel 2 die wichtigen Begriffe im Umfeld von Verkettung und digitalen Identitäten erläutert. Dabei werden die Sichtweisen verschiedener Disziplinen wie Geschichte, Soziologie, Jura, Informatik und Wirtschaftswissenschaften auf das Thema dargestellt. Kapitel 3 beschäftigt sich mit dem Status Quo hinsichtlich der Verkettung digitaler Identitäten, speziell im Verhältnis Bürger – Staat, Verbraucher – Unternehmen sowie bei Internet-Communities im Verhältnis Nutzer – Nutzer sowie Nutzer – Anbieter. In Kapitel 4 folgt eine Analyse von Techniken und Methoden bezüglich Verkettung. Vier Szenarien illustrieren in Kapitel 5, wo im Anwendungskontext heute oder auch zukünftig Verkettung eine wesentliche Rolle spielt. Den Abschluss bilden in Kapitel 6 ein Resümee sowie eine Liste von Handlungsempfehlungen.

1.1 Datenspuren im täglichen Leben

Bereits 1971, vor der Verbreitung des Internets, wurden die Auswirkungen elektronischer Datenverarbeitung auf das Leben der Betroffenen diskutiert. Steinmüller et al. betrachten die vielfältigen öffentlichen und nichtöffentlichen Bereiche, in denen Informationen über Personen verarbeitet werden und bezeichnen schon 1971 Informationssysteme als Machtfaktor für den Kundigen. Ihre Studie zeichnet ein Zukunftsbild, das längst Alltag geworden ist [Steinmüller et al. 1971, S. 49]:

„Man muss für die Zukunft von Informationssystemen von Bund, Ländern und Gemeinden ausgehen, die untereinander und mit Informationssystemen der Wirtschaft **verbunden** sind und in denen Daten mit Hilfe der bald eingeführten Personenkennzeichen technisch von jeder Stelle abgerufen werden

[1] In dieser Arbeit sind bei neutralen Nennungen von Einzelpersonen oder Personengruppen jeweils Männer und Frauen gemeint, auch wenn aus Gründen der einfacheren Lesbarkeit auf explizite Nennung der femininen Form (die Dritte, Betroffene, Nutzerin, Bürgerin, Kundin, Verbraucherin, Angreiferin etc.) verzichtet wird.

können. Auch ein Verbund privater und öffentlicher Informationssysteme erscheint nicht ausgeschlossen; mindestens ist ein Zugriff des Staates auf private Datenbanken nicht von der Hand zu weisen."[2]

Mit der zunehmenden Verbreitung des Internets verlagern immer mehr Menschen verschiedene Aspekte ihres Lebens (teilweise) in die virtuelle Welt und bauen dabei unterschiedliche digitale Identitäten auf. Solche digitalen Identitäten entstehen aber nicht nur bei der Nutzung des Internets, sondern auch bei der Verwendung technischer Geräte oder mit Chips versehener Gegenstände, die mit ihrer Umgebung kommunizieren können und dabei vielfach auch Daten über konkrete Personen erheben und speichern. Bereits *eine* digitale Identität kann eine Vielzahl an Angaben über einen Menschen beinhalten. Durch eine Verkettung verschiedener digitaler Identitäten können Informationen über eine Person zusammengeführt und relativ einfach zu umfassenden Persönlichkeitsprofilen verdichtet werden.

Zwar werden digitale Identitäten in vielen Fällen vom Betroffenen selbst wissentlich und willentlich aufgebaut und weiterentwickelt, häufig ist diesem aber auch gar nicht oder nur unzureichend bewusst, dass Daten über ihn erhoben und gespeichert werden und so digitale Identitäten entstehen. Auch wenn die Informatisierung unseres Alltags noch längst nicht abgeschlossen ist, sondern gegenwärtig erst richtig an Dynamik zu gewinnen scheint, hinterlassen wir auch heute schon täglich eine Vielzahl an digitalen Datenspuren:

Wer morgens auf dem Weg ins Büro noch schnell eine Behörde oder einen Arzt aufsucht, muss dort zum Nachweis seiner Identität oder Berechtigung oftmals Identitätsdokumente vorlegen. Beim Arzt hat die Krankenversichertenkarte schon lange den früher üblichen Krankenversichertenschein auf Papier ersetzt. Mit der Einführung der künftigen Gesundheitskarte werden auf der Karte selbst zusätzliche Informationen abgelegt werden: Obligatorisch wird dies für digitale Rezepte sein, optional können aber auch Notfalldaten auf der Karte gespeichert werden. Sofern der Patient dies wünscht, werden künftig auch die digitale Dokumentation der eingenommenen Medikamente, der elektronische Arztbrief und die elektronische Krankenakte Realität werden.

Wer eine Behörde aufsucht, um einen Antrag zu stellen, erlebt, dass dies heute vielfach nicht mehr auf Papier geschieht, sondern Daten gleich digital erhoben und gespeichert werden – ggf. muss dann noch ein Ausdruck unterschrieben werden. Im Zuge der fortschreitenden Entwicklung des E-Government wird es sogar zunehmend überflüssig, die jeweilige Behörde überhaupt aufzusuchen.

Wer im Büro für seinen Arbeitgeber im Internet recherchiert, tut dies keinesfalls unbeobachtet, da beim Provider Inhalts- und Verbindungsdaten anfallen. Welche Fachaufsätze und Patente eine Firma anfordert, gibt z.B. Hinweise auf die gerade durchgeführten Forschungs- und Entwicklungsarbeiten.

Wenn dann in der Mittagspause das Telefon privat klingelt, ergeben sich aus den beim Arbeitgeber, im Festnetz und in den Vermittlungszentralen anfallenden Verbindungsdaten sowie den daraus zu gewinnenden Interessensdaten je nach Anruf bereits aussagekräftige Bausteine für ein Persönlichkeitsbild, z.B. Konsumgewohnheiten, Freundeskreis, Tagesablauf, Kontakte mit Polizei und Gesundheitsamt.

Bei angeschaltetem Handy fallen auch ohne einen Anruf beim Mobilfunkbetreiber Daten über den Aufenthaltsort des Besitzers an. Wird das Handy zum Telefonieren, für SMS/MMS oder Internet verwendet, entstehen ähnliche Daten wie beim Telefonieren bzw. der Internetnutzung.

Wird die Mittagspause dazu genutzt, die Kantine aufzusuchen, so darf bzw. muss vielfach bereits mit elektronischen Essenskarten bezahlt werden, wobei auch wieder digitale Datenspuren anfallen.

Wer auf dem Heimweg vom Büro noch schnell im Supermarkt einkauft oder sich gar Zeit für einen Einkaufsbummel in der Innenstadt nimmt, wird dort bereits beim bloßen Besuch durch Videokameras überwacht. Bezahlt er an der Kasse, so legt er meist seine Kundenkarte vor, um Rabattprozente oder Prämienpunkte zu erhalten, und bezahlt mit EC- oder Kreditkarte. Dabei werden Kundenkarten oft von mehreren Firmen gemeinsam betrieben, die beispielsweise erheben, wann der Einkauf erfolgt und was gekauft wurde. So ergibt sich ein recht umfangreiches Bild über das Konsumverhalten des Einzelnen.

Reichte die Zeit auf dem Heimweg für den Einkaufsbummel nicht aus, so kann man dies abends am heimischen Internetrechner nachholen. Auch hier fallen die gleichen Daten wie bei der Internet-

[2] Hervorhebung durch die Verfasser dieser Arbeit.

nutzung in der Firma an. Allerdings lassen sich daraus jetzt Erkenntnisse über die privaten Interessen und das Konsumverhalten des Einzelnen gewinnen.

Doch die Internetnutzung beschränkt sich in Zeiten des Web 2.0 nicht mehr nur auf den Bereich des E-Commerce. Immer mehr Menschen verbringen einen Teil ihrer Freizeit in virtuellen Communities statt mit Freunden oder Bekannten an ihrem Wohnort. Mit anderen Mitgliedern einer Community teilen sie oft sehr private Informationen über ihr tägliches Leben und bauen dadurch eine umfangreiche digitale Identität über sich auf, die aus dem ganzen Internet abrufbar ist.

Nicht immer sind die über einen Menschen verkettbaren Daten oder die von ihm aufgebaute oder gebildete digitale Identität dabei authentisch oder aussagekräftig, denn teilweise können Datenspuren verwischt oder gefälscht werden.

Dies ist aber nicht der einzige Grund, weshalb digitale Identitäten ein falsches Bild über den Menschen vermitteln können. Selbst wenn alle Daten richtig erhoben und gespeichert werden, erhält man allenfalls einen Näherungswert über die Gewohnheiten und den Charakter der Person, deren Daten erhoben wurden: Nicht jeder, der sieben Wochen lang immer abends um sechs Uhr einkaufen war, wird dies zukünftig auch tun. Nicht jeder, der Windeln kauft, hat eigene Kinder (sondern tut dies möglicherweise für seine WG-Mitbewohnerin, weil diese nicht dazu kommt).

Die erhobenen Daten können nur mit statistischen Feststellungen in Verbindung gesetzt werden, die nach dem Gesetz der großen Zahl zwar auf die Mehrzahl der jeweiligen Referenzgruppe zutreffend sein mögen, nicht jedoch zuverlässige Aussagen über den Einzelnen ermöglichen.

1.2 Erwünschte vs. unerwünschte Verkettung

Ist Verkettung „gut“ oder „schlecht“? Diese Frage wird sich jeder stellen, der sich mit dem Phänomen der Verkettung digitaler Identitäten beschäftigt. Vor dem Hintergrund einer vernetzten Welt und der bei Staat und Wirtschaft erkennbaren Tendenz, möglichst viele Informationen über Bürger bzw. Kunden zusammenzutragen, liegt es zunächst einmal nahe, die Verkettung von Daten als ein nur bedingt beeinflussbares Risiko oder gar als unkontrollierbare Gefahr für den Betroffenen wahrzunehmen[3]. Dies gilt insbesondere dann, wenn man Verkettung aus der Sicht des Datenschutzes betrachtet und sich vergegenwärtigt, welche verborgenen Risiken und Gefahren für die informationelle Selbstbestimmung bei einer exzessiven Verkettung von Daten dem vordergründigen Nutzen einer solchen Verkettung gegenüber stehen.

Eine pauschale Bewertung von Verkettung als „schlecht“ oder „böse“ würde aber viel zu kurz greifen. Entscheidend ist zunächst einmal, aus welcher Perspektive man das Thema betrachtet. Es dürfte nämlich außer Frage stehen, dass die Verkettung von Daten aus der Sicht des jeweils Verkettenden in aller Regel gewollt sein wird. Wäre dies nicht der Fall, würde dieser die Verkettung nämlich erst gar nicht vornehmen. Aber auch aus der Sicht der Person, deren Daten verkettet werden, ist Verkettung nicht per se als negativ zu beurteilen. Vielmehr gibt es durchaus eine Reihe von Konstellationen, in denen eine Person, die von einer Verkettung betroffen ist, dies wegen der hieraus erwachsenden Möglichkeiten als vorteilhaft erachtet. In solchen Fällen ist also eine Verkettung auch aus Sicht des hiervon Betroffenen erwünscht.

Da Verkettung oft zugleich Chancen und Risiken mit sich bringt, wird es in vielen Fällen von der Sichtweise und den Präferenzen der jeweils betroffenen Personen abhängen, ob sie erwünscht oder unerwünscht ist. So werden manche Menschen die Verkettung ihrer Daten im Rahmen von Bonusprogrammen wegen der in diesem Zusammenhang gewährten Vergünstigungen als positiv beurteilen, während andere solche Programme strikt ablehnen werden, weil sie hierin eine (potenzielle) Einschränkung ihrer Privatsphäre sehen.

Es erscheint insofern als sinnvoll, im Zusammenhang mit Verkettung nicht Begriffe wie „gut“ oder „böse“ zu bemühen, sondern zwischen individuell bzw. kollektiv erwünschter und unerwünschter Verkettung zu differenzieren. Verkettung ist also zunächst einmal ein wertfreier Begriff und kann in

[3] Die Begriffe Risiko und Gefahr unterscheiden sich nach dem diesen Ausführungen zugrundeliegenden Verständnis insoweit, als ein Risiko beeinflussbar ist, während dem Betroffenen bei einer Gefahr die Möglichkeit fehlt, diese zu beeinflussen (vgl. [Luhmann 1991, S. 30 f., 112 ff.]).

einem Kontext erwünscht, in einem anderen hingegen unerwünscht sein. Gleiches gilt, wenn Verkettung(en) aus unterschiedlichen Perspektiven betrachtet werden. Während ein „Verketter“ im Regelfall ein vitales Interesse daran haben dürfte, je nach Gusto Daten miteinander verketten zu können, erscheint es aus der Perspektive der Personen, deren Daten verkettet werden sollen, als erstrebenswert, wenn nicht sogar unabdingbar, Verkettungen steuern und kontrollieren zu können. Zumindest wäre gegenüber den Betroffenen Transparenz über die geplanten (und möglichen) Verkettungen sowie ihre Auswirkungen geboten. Es sollte folglich – im Idealfall – stets möglich sein, Verkettung(en) unter Bedingungen stellen zu können: Die betroffenen Personen sollten die Verkettung ihrer Daten beherrschen können und nicht ihrerseits mittels von ihnen nicht kontrollierbarer Verkettungen beherrscht, d.h. in ihrer Rechtewahrnehmung (potenziell) beeinträchtigt, werden. Dies gilt umso mehr vor dem Hintergrund, dass es sich bei „Verkettern“ im Wesentlichen um staatliche oder private Organisationen handeln wird, die den von der Verkettung betroffenen Personen zumeist in vielerlei Hinsicht – technisch, pekuniär etc. – überlegen sein werden.

In manchen Zusammenhängen ist es besonders wichtig, Verkettungen steuern zu können, weil diese gravierende Folgen nach sich ziehen können. Man denke etwa an eine Person, die sich bei den Anonymen Alkoholikern engagiert und in diesem Zusammenhang unter Pseudonym einen Blog im Internet betreibt. Für diese Person kann es in vielerlei Hinsicht von elementarer Bedeutung sein, dass dieses Pseudonym nicht mit ihrer Person in Verbindung gebracht werden kann. Sollte diese Verkettung dennoch vorgenommen werden, besteht die Gefahr, dass die Person wegen ihrer (vermeintlichen) Alkoholkrankheit in den unterschiedlichsten Kontexten Ablehnung erfährt.[4]

Damit bleibt an dieser Stelle Folgendes festzuhalten: Verkettung von Identitäten oder sonstigen Daten ist zunächst einmal ein wertfreier Begriff und kann je nach Einzelfall erwünscht oder unerwünscht sein. Unerwünschte Verkettungen können in machen Fällen gravierende Auswirkungen auf die soziale Reputation einer Person haben. Nicht zuletzt deshalb besteht eine Notwendigkeit dafür, Verkettungen unter Bedingungen stellen zu können.

[4] Dabei wird typischerweise nicht nur diese Facette der betroffenen Person abgelehnt, sondern die Person als Ganzes. Dies gilt insbesondere dann, wenn die Eigenschaft oder das Verhalten der betreffenden Person anhand des binären Systems der Moral (Achtung/Missachtung) bewertet wird. Die aus einer moralischen Beurteilung eines Verhaltens resultierende Achtung oder Missachtung einer Person bleibt nämlich in aller Regel nicht auf diesen einen Aspekt der Person beschränkt, sondern bezieht sich stets auf die Komplettperson, die als Ganzes geachtet oder missachtet wird (vgl. [Fuchs 2007]).

2 Grundlagenteil

2.1 Einführung

In diesem Abschnitt wird zunächst das nötige Grundlagenwissen zu Begriffen sowie grundsätzlichen Zusammenhängen vermittelt, das für das Verständnis der weiteren Ausführungen in dieser Arbeit benötigt wird. Hiernach folgen grundsätzliche Ausführungen zum Thema Verkettung digitaler Identitäten aus der Perspektive verschiedener fachlicher Disziplinen (interdisziplinärer Ansatz). Im Einzelnen handelt es sich dabei um Ausführungen zu historischen, soziologischen, juristischen, technischen und ökonomischen Grundlagen.

2.2 Verkettung digitaler Identitäten – die Grundlagen

Dieser Abschnitt bildet die Basis für das Thema Verkettung, indem die wesentlichen Begriffe eingeführt werden. Die Relevanz von Verkettung wird deutlich anhand aufgezeigter Trends beim Weg in die Informationsgesellschaft. Anschließend werden digitale Identitäten und ihre Eigenschaften, insbesondere im Hinblick auf Verkettungsmöglichkeiten, analysiert. Im Modell der Informationsanreicherung wird Verkettung in den Kontext gesetzt, und wesentliche Rollen im Umfeld von Verkettung werden mit ihren Aufgaben und Einflussmöglichkeiten erläutert. Da Verketten digitaler Identitäten in der Regel eine Aktion im Vorfeld von Entscheidungen und Folgen für Betroffene darstellt, werden auch die für die Privatsphäre der Betroffenen relevanten Identitätsattribute näher betrachtet.

2.2.1 Verkettung von Daten

Verkettung von Daten bedeutet „In-Beziehung-Setzen“ dieser Daten. Aus Sicht eines Individuums geschieht dies ständig: Es gehört zum Leben dazu und macht sogar große Teile dessen aus, dass man selbst seine eigenen Aktionen in Beziehung setzt und dies ebenso mit den Aktionen anderer, die auf einen wirken, tut. Ein solches Verketten ist eine grundlegende Notwendigkeit für ein Lernen, d.h. ein Weiterentwickeln der eigenen Fähigkeiten und der Persönlichkeit aufgrund der gemachten Erfahrungen. Auch ist Verkettung von Aktionen anderer wichtig, damit man ihr Verhalten für die Zukunft prognostizieren und fundiertes Vertrauen in andere entwickeln kann.

Auch die Gesellschaft als Ganzes hat Interesse an Verkettung, denn ohne ein Erinnern und Einordnen der historischen Informationen wäre Kultur nicht denkbar. Dies zeigen auch die standesamtlich geführten Personenstandsregister, die Geburten, Heiraten und Sterbefälle einer Gemeinde bzw. einer Stadt über den Tod der Betroffenen hinaus speichern. Ebenso spielt Verkettung für Organisationen eine Rolle, z.B. um personalisierte Dienste anzubieten, eine stärkere Kundenbindung zu erreichen oder um mit Hilfe von Reputationsinformationen auf Basis der vergangenen Transaktionen zukünftiges Verhalten zu prognostizieren.

Verkettung setzt das Vorhandensein von Daten voraus. Diese Daten können speziell zu bestimmten Zwecken erhoben worden sein, z.B. in staatlichen Registern gespeicherte Informationen, oder aber sie fallen quasi nebenbei an, z.B. Datenspuren, die bei Nutzeraktionen im Internet entstehen.

Im Folgenden werden die wichtigsten Begriffe im Umfeld von Verkettung definiert und zueinander in Beziehung gesetzt:

- **Verkettung von Daten:** Das In-Beziehung-Setzen oder Zusammenführen dieser Daten[5]. Dies geschieht üblicherweise in Hinblick auf einen vordefinierten Zweck, z.B. um Daten einer Person oder umgekehrt eine Person zugehörigen Daten zuzuordnen oder um Daten durch Profilbildung zu gruppieren. Bei den Akteuren, die das Verketten durchführen, handelt es sich um natürliche oder juristische Personen oder um Computer. Verkettung kann sich z.B. darin äußern, dass die Daten in derselben Datenbank gespeichert werden und mit Hilfe von Datenbankanfragen verknüpft ausgegeben werden.

[5] Dies muss nicht direkt, sondern kann auch transitiv in mehreren Schritten geschehen.

- **Verkettbarkeit von Daten:** Die Möglichkeit der Verkettung dieser Daten. Verkettbarkeit für eine Person oder einen Computer liegt typischerweise dann vor, wenn verschiedene Daten dieselben Kennungen (Identifier) aufweisen und diese für die Person oder den Computer sichtbar sind. Verkettbarkeit hängt also nicht nur ab von den Daten selbst, sondern auch von den Möglichkeiten des Zugriffs und der Perspektive des Verketters.[6]

- **Unverkettbarkeit von Daten[7]:** Die Unmöglichkeit der Verkettung dieser Daten. Wiederum kann man hier die Perspektive eines potenziellen Verketters einführen, für den die Daten nicht (oder nicht sinnvoll für den gewählten Zweck) verkettbar sind. Im Gegensatz zu den anderen hier genannten Eigenschaften Verkettbarkeit und Entkettbarkeit genießt Unverkettbarkeit einen Sonderstatus, da dieser Begriff in den ISO-standardisierten Common Criteria als Schutzziel der Klasse „Privacy" definiert ist, zu der auch Anonymität, Pseudonymität und Unbeobachtbarkeit gehören.[8] Absolute Unverkettbarkeit, die für alle potenziellen Verketter gilt, ist in der Praxis oft nur schwer oder gar nicht zu erreichen. Daher zielen alternative Definitionen von Unverkettbarkeit darauf, dass ein potenzieller Verketter durch eine Beobachtung keine neuen Erkenntnisse über eine etwaige Zugehörigkeit von Daten zueinander (bzw. zur selben Person) gewinnt [Pfitzmann/Hansen 2007][9].

- **Entkettung von Daten:** Das Herauslösen von einzelnen Daten aus einem Datenbestand, d.h. aus bereits verketteten Daten. Die Verkettung wird dadurch im Nachhinein gelöst. Dies kann durch Trennen der Daten in verschiedene Datenbanken geschehen, die sich in ihren Zugriffsberechtigungen unterscheiden. Auch bewirkt beispielsweise ein Löschen von Einzelkomponenten (oder das Sperren des Zugriffs darauf) eine nachträgliche Reduzierung des Datenprofils, die der Entkettung zugerechnet werden kann. Verringert sich für einen potenziellen Verketter die Gewissheit darüber, ob bestimmte Daten tatsächlich in Beziehung stehen oder nicht, hat dies einen entkettenden Effekt. Dies ließe sich beispielsweise durch versehentliche Missinformation oder gezielte Desinformation erreichen.
  Entkettung bedeutet nicht zwangsläufig, dass die Daten für den Entketter nicht mehr verkettbar sind. In der Regel ist ein nachträgliches Herauslösen von Daten derart, dass tatsächlich keine Verkettung mehr möglich ist, technisch oder auch psychologisch kaum zu garantieren.

---

6 Es sei hier angemerkt, dass nach dieser Definition die verketteten Daten nicht zwangsläufig tatsächlich in Beziehung gestanden hatten, bevor sie verkettet wurden. Beispielsweise könnten Daten von verschiedenen, überhaupt nicht miteinander in Beziehung stehenden Personen irrtümlicherweise zusammengeführt werden – unter der fälschlichen Annahme, es handele sich um ein- und dieselbe Person.

7 Ein etwa korrespondierender Begriff „Unverkettung" ist nicht sinnvoll, weil „mangelndes Verketten" keinen aktiven Prozess darstellt.

8 „[Unlinkability] ensures that a user may make multiple uses of resources or services without others being able to link these uses together. [...] Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system." (ISO/IEC 15408:2005). Der Fokus dieser Definition liegt auf der Verkettbarkeit mehrerer Nutzeraktionen, die für andere ausgeschlossen sein soll.

9 Nach [Pfitzmann/Hansen 2007] ist „unlinkability" folgendermaßen definiert:
„Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not." Hierbei sind zwei Aspekte hervorzuheben:
1. Im Mittelpunkt dieser Definition steht das Wissen eines Angreifers darüber, ob zwei Dinge in Beziehung stehen oder eben gerade nicht. „Unlinkability" drückt aus, dass der Angreifer dieses Wissen nicht (oder nicht mit ausreichender Gewissheit) hat. Weiß der Angreifer beispielsweise, dass zwei Dinge *nicht* in Beziehung stehen, ist nach dieser Definition „unlinkability" *nicht* gegeben. Stattdessen läge „linkability" vor.
2. Diese Definition ist durch das „sufficiently" parametrisiert: Selbst wenn ein Angreifer durch seine Beobachtungen einen Informationsgewinn erzielt, muss es für ihn auch danach hinreichend ungewiss sein, ob zwei Dinge in Beziehung stehen oder nicht. Um den ausreichenden Grad an Ungewissheit bestimmen zu können, muss – je nach Perspektive und Kontext – dafür ein Schwellwert definiert werden.

Als Vergleich hier die Definition zu „linkability" nach [Pfitzmann/Hansen 2007] als Negation von „unlinkability":
„Linkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not."
Wird in dieser Arbeit die für eine technische Diskussion besser geeignete Definition nach [Pfitzmann/Hansen 2007] verwendet, wird dies jeweils angegeben.

- **Entkettbarkeit von Daten:** Die Möglichkeit des Entkettens in Bezug auf diese Daten.
- **Unentkettbarkeit von Daten:** Nicht üblich, aber logisch formulierbar ist dieser Begriff, der für die Unmöglichkeit einer Entkettbarkeit steht.

Die folgende Tabelle 1 stellt diese Begriffe im Überblick dar:

	Tatsächliche Aktion	**Möglich**	**Nicht möglich**
Verketten?	Verkettung	Verkettbarkeit	Unverkettbarkeit
Verkettetes wieder entketten?	Entkettung	Entkettbarkeit	Unentkettbarkeit

Tabelle 1: Wesentliche Begriffe im Umfeld von Verkettung

Wichtig ist jeweils, inwieweit die Eigenschaften Verkettbarkeit, Unverkettbarkeit oder Entkettbarkeit garantiert, für wahrscheinlich oder unwahrscheinlich gehalten oder lediglich nicht ausgeschlossen werden können.

Will man für zwei Datenbestände Unverkettbarkeit innerhalb eines IT-Systems erreichen, darf es für niemanden möglich sein, eine Kette zwischen den entsprechenden Datenbeständen zu konstruieren. Die Möglichkeit von nur einer Kette hätte eine allgemeine Unverkettbarkeit bereits ausgeschlossen.

Wünscht man Verkettbarkeit von Datenbeständen, ist mindestens eine Kette erforderlich, und diese sollte verfügbar sein, sobald sie benötigt wird, und Integrität gewährleisten.

2.2.2 Der Weg in die Informationsgesellschaft

Mit Einführung von Computern, die Speicher und Verarbeitungslogik bereitstellen und Daten über Netze austauschen können, ist eine Verkettung von Daten sehr viel einfacher geworden, als es vorher war. Kennzeichnend für die digitale Welt, auf der die Informationsgesellschaft fußt, sind die folgenden Trends:

- **Zunehmende Speicherkapazität und Verarbeitungsleistung:**
  Festplatten im Bereich von 500 GB werden heute schon für unter 100 EUR angeboten, und die gängigen Speicherkapazitäten nehmen weiter zu. Dies gilt auch für die Rechengeschwindigkeit der Prozessoren.
- **Miniaturisierung:**
  Datenverarbeitung findet nicht nur in Rechenzentren, auf Arbeitsplatzcomputern und tragbaren Notebooks oder handflächengroßen Personal Digital Assistants und Handys statt, sondern Transponder sind teilweise kleiner als 1 mm³. Digitale Fotoapparate oder Videokameras werden heute standardmäßig in Handys untergebracht oder können im ferngesteuerten Modellflugzeug mitfliegen.
- **Sensorik:**
  Für den Bereich der Biometrie, aber auch für die Messwerttechnik stehen intelligente Sensoren zur Verfügung, die die Umgebung erkennen und bewerten können. Überwachungstechniken werden zunehmend nachgefragt.
- **Vernetzung von Computern über Internet und Mobiltelefonie:**
  Computer sind in der Regel in der Lage, miteinander zu kommunizieren – per Kabel oder Funk. Internetnutzung ist für viele Menschen selbstverständlich. Sprach- und Datenkommunikation wachsen zusammen: Mobiltelefone werden auch zur Datenübertragung eingesetzt; Voice-over-IP ermöglicht ein Telefonieren über das Internet.
- **Ubiquität von Computern:**
  In vielen Alltagsgegenständen wie dem Auto oder einer Waschmaschine befinden sich heute schon Prozessoren. Die neue Generation von Reisepässen ist mit RFID-Chips ausgestattet.

Die Allgegenwärtigkeit von Computern, die spontan miteinander kommunizieren, ist in ersten Modellen von intelligenten Häusern schon Wirklichkeit.

- **Intransparenz der Verarbeitungsprozesse und Datenspuren:**
  Kaum jemand überblickt noch die um einen herum stattfindende Datenverarbeitung – zum einen sind die IT-Systeme zunehmend komplex, zum anderen erfährt man häufig auch gar nicht, was jeweils an Daten übertragen oder verarbeitet wird. Den meisten Nutzern ist nicht bewusst, dass sie im Internet oder bei der Handynutzung Datenspuren hinterlassen
- **Mängel in der Datensicherheit:**
  Bei der hohen Entwicklungsgeschwindigkeit im Computer- und Telekommunikationsbereich hält die Integration von angemessenen Sicherheitsmaßnahmen nicht Schritt. Täglich werden neue Sicherheitslücken bekannt, Viren und Trojanische Pferde verbreiten sich, Nutzer lassen sich von Phishing-Websites täuschen.

Ein Einsatz von Computern ist heute in nahezu allen Lebensbereichen möglich. Es verarbeiten nicht mehr nur große Rechenzentren Daten, wie dies in der Anfangszeit der elektronischen Datenverarbeitung der Fall war, sondern mittlerweile verfügen fast alle Menschen in der Informationsgesellschaft über eigene Computer, die als Speicher- und Verkettungsmaschinen für beliebige digitale Daten dienen können.

Aufgrund dieser Trends wird es immer wichtiger, Verkettung von Daten unter gesellschaftlich akzeptierte Bedingungen zu stellen und diese auch durchzusetzen.

2.2.3 Digitale Identitäten

In dieser Arbeit steht die Verkettung digitaler Identitäten im Vordergrund: Digitale Identitäten repräsentieren die Nutzer in der Informationsgesellschaft. Solche digitalen Identitäten bestehen aus technisch abgebildeten Attributen der Nutzer, den Identitätsdaten[10]. Dazu gehören z.B. Adressdaten, biometrische Daten, Vorlieben etc. Nicht immer liegen die Daten von Anfang an computerisiert vor, sondern es kann auch sein, dass sie erst digitalisiert werden müssen wie z.B. bei einem Scannen von Dokumenten oder Aufzeichnen und Umwandeln von Tönen.

2.2.3.1 Identität, digitale Identität sowie Teilidentitäten

Geht man von der Identität eines Menschen mit all ihren Facetten aus, ist dessen *digitale Identität* die Untermenge dessen, was technisch abgebildet wird, z.B. was Sensoren messen oder was man in Form von Texten, Bildern oder Geräuschen zu Identitätsattributen speichert.[11] Heutzutage – und vermutlich auch noch in der überschaubaren Zukunft – ist nirgends das Gesamtbild der digitalen Identität eines Menschen zugreifbar, sondern typischerweise findet man an vielerlei Stellen Teile davon vor, die sog. digitalen *Teilidentitäten*, die wiederum Untermengen der digitalen Identität sind. Da stets durch den Sinnzusammenhang klar ist, ob die gesamte digitale Identität oder die Teilidentitäten gemeint sind, verwenden wir im Folgenden den Begriff der digitalen Identitäten auch für die digitalen Teilidentitäten. Abbildung 1 veranschaulicht die gerade vorgestellten Begriffe und ihre Beziehungen zueinander.

[10] Der Begriff „Identitätsdaten“ wird manchmal beschränkt auf diejenigen personenbezogenen Daten, anhand derer eine Person identifiziert werden kann und/oder für einen bestimmten Lebens- oder Sachbereich auf Eigenschaften dieser Person rückgeschlossen werden kann. In dieser Arbeit wird der Begriff etwas weiter gefasst: Identitätsdaten sind Daten einer digitalen Teilidentität. Sie können die oben genannten Eigenschaften aufweisen, aber ebenso ist es möglich, dass ein Beobachter allein daraus keine Informationen über einen Personenbezug oder die Person selbst gewinnt. Gegebenenfalls ergibt sich diese Information nach einer Verkettung von Identitätsdaten mit weiteren Daten.

[11] Nach G. H. Mead besteht die Identität eines Menschen aus dem „I“ und dem „Me“, wobei das „Me“ all diejenigen Identitätsattribute umfasst, die sich technisch operationalisieren lassen [Mead 1934]. In diesem Kontext wären dies also alle möglichen technischen Erfassungen von Identitätsattributen.

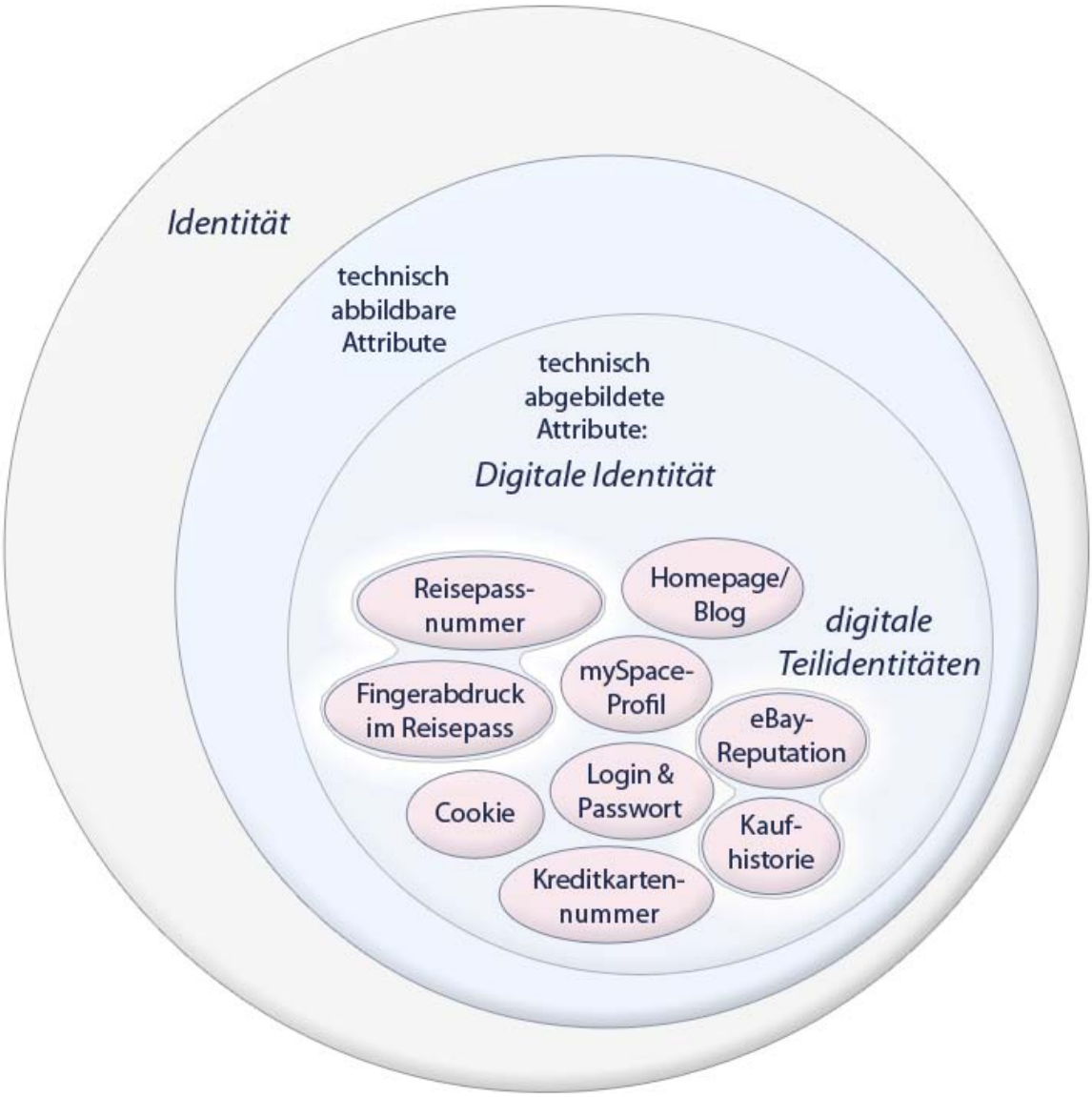


Abbildung 1: Identität, digitale Identität und digitale Teilidentitäten

2.2.3.2 Informationsquellen

Informationsquellen für digitale Identitäten können vielfältig sein – teils hängen sie unmittelbar vom Betroffenen ab, ggf. in einer aktiven Rolle, teils prägen Dritte, wovon der Betroffene nicht unbedingt etwas weiß, das Bild vom Betroffenen. Insbesondere können sich die digitalen Identitäten aus den folgenden Informationen zusammensetzen, die unmittelbar Bezug zum Betroffenen haben, bei denen entweder er selbst oder Dritte als Informationsquelle dienen (siehe Tabelle 2):

	Informationsquelle: der Betroffene selbst	**Informationsquelle: Dritte**
Physiologische oder genetische Merkmale	z.B. gemessen von Sensoren oder Analysemethoden, die Auskunft geben etwa zu Größe, Gewicht, Haut-, Augen- oder Haarfarbe, DNA oder anderen physiologischen biometrischen Merkmalen	z.B. bei DNA-Untersuchungen von Verwandten, die auch genetische Informationen des Betroffenen preisgeben oder zumindest nahelegen
Äußerungen	z.B. durch Einträge in Webformularen bei angelegten Accounts, eine eigene Homepage, selbst angelegte Profile in sozialen Netzwerken oder auch unmittelbar in einer Kommunikation wie etwa E-Mail- oder Telefonäußerungen	z.B. durch Äußerungen mit Einschätzungen zum Betroffenen, durch Bewertungen in einem Reputationssystem oder durch ausgestellte Bescheinigungen wie Geburtsurkunde oder Zeugnisse
Handlungen	z.B. etwas kaufen, sich sportlich betätigen oder im Verkehr einen bestimmten Weg wählen	z.B. Geschenk für den Betroffenen besorgen (enthält Aussage zum angenommenen Interesse) oder mit Vollmacht in seinem Auftrag handeln
(Potenzielle) Kontakte	z.B. Einträge von Namen oder Telefonnummern anderer im Adressbuch oder die zuletzt angesurften Webseiten	z.B. Kommunikationsadressen des Betroffenen beim Dritten gespeichert oder durch ihn getätigte Kontaktanfrage in einem sozialen Netzwerk; absichtliches Vermeiden der Kontaktaufnahme

Tabelle 2: Informationsquellen – unmittelbarer Bezug zum Betroffenen

Die *physiologischen oder genetischen Merkmale* betreffen direkt den Körper des Betroffenen oder auch DNA-basierte Persönlichkeitsmerkmale, die durchaus auch bestimmte Verhaltensweisen beeinflussen können. *Äußerungen* werden aktiv abgegeben, z.B. mündlich oder schriftlich, und können Selbst- oder Fremdeinschätzungen beinhalten. *Handlungen* sind ebenfalls Aktionen, die üblicherweise bewusst geschehen. *Kontakte oder potenzielle Kontakte* zeigen ein Interesse am anderen; dies ist nicht unbedingt beidseitig. Die vier Kategorien sind in der Praxis nicht ganz trennscharf, aber zeigen die zumeist wichtigsten Bereiche auf, die als Informationsquellen dienen können.

Neben den genannten (primären) Informationsquellen, die selbst Informationen generieren, müssen auch sekundäre Quellen in Betracht gezogen werden, die erhaltene Informationen lediglich weiterleiten. Selbst wenn ein aktives Äußern oder Handeln oder auch bewusstes Weiterleiten von Informationen gegeben ist, heißt dies nicht, dass dem Betroffenen bewusst ist, wem dies als Informationsquelle dienen und welche Aussagekraft damit verbunden sein mag.

Während der *unmittelbare Bezug* zum Betroffenen direkt mit ihm in Zusammenhang gebracht wird, ist dies beim *mittelbaren Bezug* nur indirekt der Fall, z.B. indem nicht der Betroffene als Person, sondern eine Gruppe, der er zuzuordnen ist, im Fokus steht, indem Annahmen über ihn extrapoliert werden oder indem Kontakte über mehrere Ecken ausgewertet werden. All diese Fälle sind mit einem gewissen Maß an zusätzlicher Ungewissheit verbunden, ob die aus diesen indirekten Informationsquellen gewinnbaren Schlüsse wirklich Bestand haben (siehe Tabelle 3).

	Informationsquelle: Dritte
Äußerungen	z.B. Äußerungen nicht über ein Individuum, sondern über eine Gruppe, der der Betroffene (möglicherweise) angehört
Handlungen	z.B. wenn das Verhalten in bestimmten Aspekten ähnlich dem des Betroffenen ist, kann ein „statistischer Zwilling“ angenommen werden, dessen beobachtetes Verhalten in anderen Aspekten für den Betroffenen extrapoliert wird
(Potenzielle) indirekte Kontakte	z.B. „Friend-of-a-Friend“, d.h. ein nicht-unmittelbarer Kontakt in einem sozialen Netzwerk, sondern transitiv über mehrere Kontakte

Tabelle 3: Informationsquellen – mittelbarer Bezug zum Betroffenen

Bei all diesen Informationsquellen kommen neben den eigentlichen inhaltlichen Aussagen und Beobachtungen wenigstens Kontextdaten (zumindest Ort- und Zeitinformationen) hinzu. Darüber hinaus sind Datenspuren typisch für die digitale Welt, die bedingt durch die Implementierung[12] der technischen Protokolle anfallen, z.B. die Informationen über die IP-Adresse oder die Funkzelle. Auch können Inhaltsdaten, Kontextdaten und technische Datenspuren einzeln oder in Kombination weiteren Informationsgehalt bieten.

2.2.3.3 Personenbezug für wen?

Auch wenn sich eine digitale Identität stets auf eine Person bezieht[13], sind doch die Daten aus Sicht eines Dritten so lange nicht personenbezogen gemäß der Definition in den Datenschutzgesetzen, wie für ihn die dahinter stehende Person nicht bestimmbar ist.[14] Der Personenbezug ist ein wichtiges Kriterium bei der Analyse von Verkettung und ihren Auswirkungen. Es ist offensichtlich, dass das In-Beziehung-Setzen von Daten und einer Person das Herstellen eines Personenbezugs beschreibt. Dies können z.B. beobachtete Attribute sein, die mit dem vollen Namen des Nutzers verkettet werden. Eine andere Art von Verkettung reichert Daten an, z.B. durch Zusammenführen von Daten, die unter demselben Pseudonym offenbart wurden. In vielen Fällen wird auch ein pseudonymes Profil so aussagekräftig sein, dass der unmittelbare Personenbezug gegeben ist.

Personenbezogene Daten sind in vielen Fällen als sensibel einzustufen. Das Datenschutzrecht kennt Sensibilität insbesondere bei den so genannten besonderen Arten von Daten (vgl. § 3 Abs. 9 BDSG), nämlich Daten über rassische und ethnische Herkunft, die politische Meinung, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit und das Sexualleben. Aber auch umfassende Persönlichkeits-, Interessens- oder Bewegungsprofile über eine Person sind sensibel, da sie eine Vielzahl von Auswertungen ermöglichen, die von dem Betroffenen als invasiv und Eingriff in seine Privatsphäre wahrgenommen werden können. Spürt man beim Betroffenen sogar auf, wofür er besonders empfänglich ist oder wo er möglicherweise labile Züge aufweist, kann man hier manipulativ wirken: um seine Stimme bei der nächsten Wahl zu erhalten oder schlicht um ihm Waren zu verkaufen und ihn an die Herstellerfirma zu binden.

2.2.3.4 Übergang zur traditionellen Welt

Die digitale Welt enthält zwar keine physischen Körper aus Fleisch und Blut, aber dies verhindert nicht missbräuchliche Nutzungen von Daten, die innerhalb des digitalen Bereichs oder sogar in der „echten Welt“ Auswirkungen auf das Leben der Betroffenen haben. Die Übergänge sind fließend:

[12] Häufig bedingt durch die *naive* Implementierung.
[13] Auch wenn die Person sich ihrer digitalen Identität nicht in jedem Fall bewusst ist.
[14] Vgl. auch die Ausarbeitungen zum Konzept personenbezogener Daten der europäischen Art. 29-Datenschutzgruppe [Art. 29-Datenschutzgruppe 2007].

- Bei Biometrie werden körperliche Merkmale digital erfasst. Auch wenn im Vordergrund des Biometrie-Einsatzes die Funktion der Authentisierung stand, können die digitalen Daten zusätzliche Informationen – z.B. medizinischer Art – enthüllen (siehe auch Abschnitt 4.3.2).
- Aus einer DNA-Analyse, die sich digital speichern lässt, ergibt sich nicht nur das Geschlecht, sondern man erhält auch Hinweise auf bestimmte Krankheitswahrscheinlichkeiten und eingeschränkt auch auf das Aussehen einer Person.
- Verhaltensbasierte Sensorauswertungen sollen zunehmend zwischen erwünschtem und unerwünschtem (oder unauffälligem und auffälligem) Verhalten unterscheiden. Dies führt bei Menschen, denen dies bewusst ist, zu Verhaltensanpassungen.
- Beim Identitätsdiebstahl tritt ein Dritter unter dem Namen und den Adressen des Betroffenen auf, ohne dass dieser es so wollte. Es ist für den Betroffenen aufwändig, bei allen Aktionen des Dritten richtig zu stellen, dass sie ihm nicht zuzurechnen sind, und ggf. getätigte Transaktionen rückabzuwickeln. Hat sich der Dritte unter dem Namen des Betroffenen regelwidrig verhalten, hat möglicherweise die Reputation des Betroffenen schon derart Schaden erlitten, dass er sich gar nicht mehr Gehör verschaffen kann, z.B. wenn eine E-Mail-Adresse wegen Spam-Versands auf Sperrlisten gerät, die im Internet weiterverteilt werden.
- Je nach Surf- und Klickverhalten auf einer Website können einem unterschiedlichen Preise für Produkte offeriert werden, weil Analysen darüber Auskunft geben, inwieweit Kategorien wie „Schnellklicker“ oder „Warenkorbabbrecher“ bereit sind, höhere Preise zu zahlen.
- Scoring von digital gespeicherten Daten prägt typischerweise die Entscheidung für oder gegen eine Kreditvergabe oder ein Zustandekommen eines Handyvertrags, wobei es vorkommt, dass auf inkorrekten Basisdaten oder mit qualitativ unzureichenden Scoring-Algorithmen gearbeitet wird.
- Bei der Patientenbetreuung kommen ebenfalls digitale Systeme zum Einsatz, die auf der gegebenen Datenbasis über die Gabe von Medikamenten entscheiden. Die Mensch-Maschine-Schnittstelle wird dabei immer unmittelbarer: Im Fall von Implantaten und Prothesen bis hin zum „Body Area Network“[15] können Sensor-Aktor-Kopplungen Körperfunktionen messen und dann direkt auf den Menschen wirken.

2.2.4 Verkettung im Kontext

Prinzipiell kann alles mit allem in Beziehung gesetzt werden; jedoch verfolgen üblicherweise diejenigen, die verketten, dabei bestimmte Zwecke, die auch die Methodik vorgeben, auf welche Weise das vorhandene Datenmaterial verkettet werden soll. Gleichheit von Namen, Pseudonymen, Adressen oder anderen Kennungen sind nicht die einzigen Verkettungsmöglichkeiten; ebenso können etwa Daten, die sich in Zeit- und Raumkoordinaten ähneln, zusammengeführt werden, z.B. um Bewegungsmuster ausfindig zu machen.

2.2.4.1 Modell der Informationsanreicherung

Um sowohl die Vorbedingungen als auch die möglichen Folgen von Verkettung zu verdeutlichen und die Einbindung möglicher Akteure zu veranschaulichen, führen wir ein allgemeines Modell für Informationsanreicherung ein, das in Abbildung 2 dargestellt wird.

[15] http://www.aerzteblatt.de/v4/archiv/artikel.asp?id=31948 (letzter Zugriff im Oktober 2007).

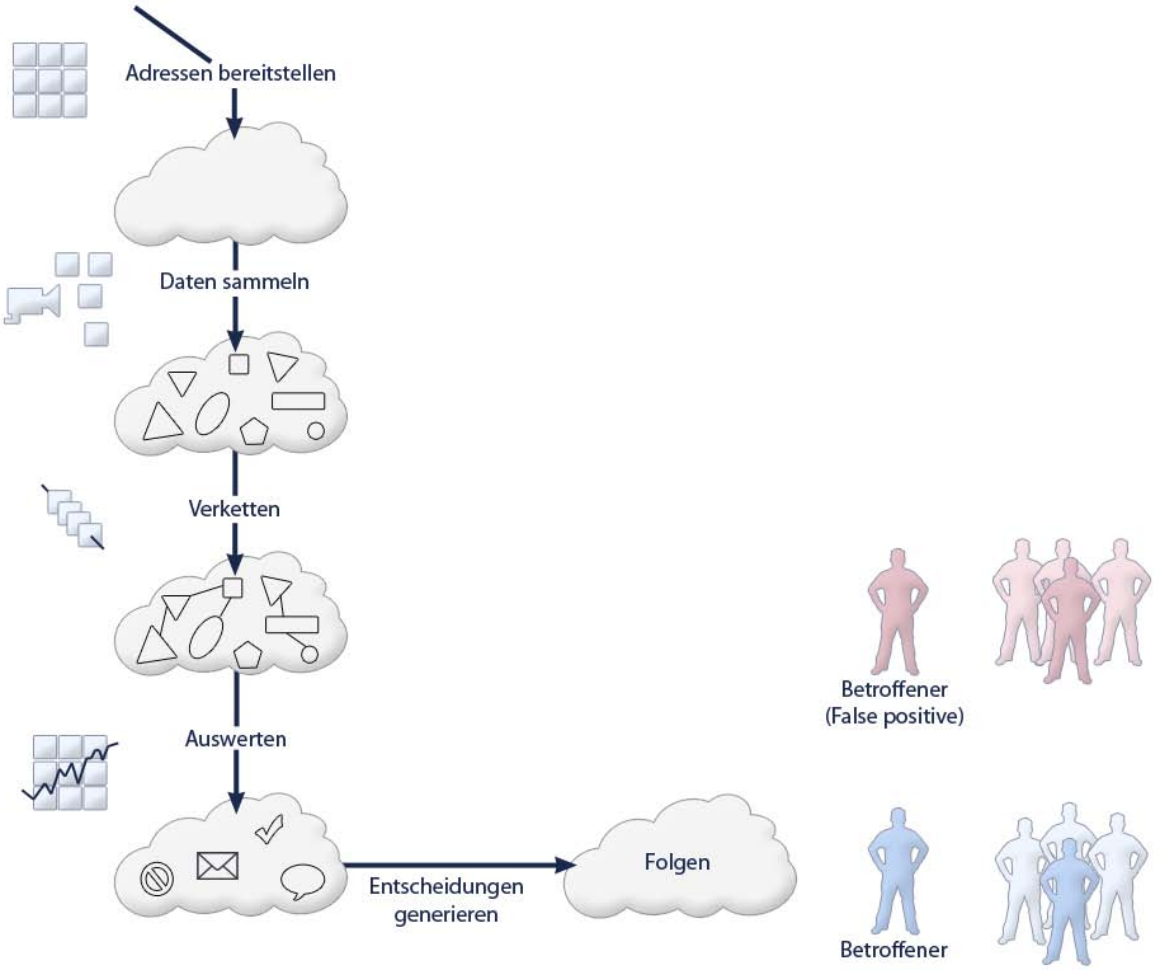


Abbildung 2: Workflow der Informationsanreicherung

1. Vorbereitung: Adressen bereitstellen

Vorausgesetzt wird das Vorhandensein von Datenmaterial. In Bezug auf digitale Identitäten sind dies sog. Attribute. Beispiele für Attribute sind „weiblich“, „1,68 m groß“, „hat rote Jacke an“, „mag Jazz“, „ist Single“. Zu diesen Attributen gehören auch die Adressen, die eindeutig für einen definierten Bereich sind.[16] Dies können Kommunikationsadressen sein wie eine IP-Adresse oder ein (eindeutiger) Name, der dazu geeignet ist, den Betroffenen anzusprechen oder auch mit einem Dritten über ihn zu reden. Der Aufbau der Adressen und ihre Funktionalität im jeweiligen System werden durch ein Adressschema spezifiziert, das ein *Adressschema-Provider* zur Verfügung stellt. Die Zuordnung von Adressen zu Personen oder Computern erfolgt durch *Adress-Provider,* die mit den Adressschema-Providern identisch sein können. Eine Adresse ist ein zur Verkettung geeignetes Attribut, denn sie ist eindeutig in ihrem Geltungsbereich.

2. Datensammlung

Wer Zugriff auf Daten hat, kann sie sammeln, d.h. erheben und speichern. Solche *Datensammler* können der Betroffene oder einer seiner Kommunikationspartner sein, es kann sich jedoch auch um private oder professionelle Beobachter handeln. Das Beobachten kann rein technisch geschehen, z.B. durch Sensoren, die alle möglichen Merkmale messen und analysieren können wie etwa Farben und Formen, Bewegungen, Temperatur oder neuerdings sogar Gerüche. Auch die Analyse von Logfiles als Teil der Datenspuren läuft auf der technischen Ebene ab.

[16] Siehe auch die entsprechenden Ausführungen im Abschnitt 2.3.2.2 aus soziologischer Sicht.

Je mehr (möglichst authentische) Daten beobachtet werden können, je mehr Lebensbereiche sie abdecken und je mehr (sensible) Informationen sie enthalten, desto aussagekräftiger können auch die gesammelten Daten sein. Mächtige Beobachter sind in der Regel Personen oder Organisationen, die an zentraler Stelle für den Betroffenen Gateway-Leistungen anbieten, d.h. Anfragen oder Verbindungsaufbauersuche aufnehmen und weiterleiten. Dies gilt auf jeden Fall dann, wenn die Kommunikation unverschlüsselt abläuft, doch auch bei Verschlüsselung können viele aussagekräftige Verbindungsdaten anfallen. Beispiele für potenziell mächtige Beobachter sind nicht nur etwa Geheimdienste, sondern auch in der herkömmlichen Welt Butler oder Mitbewohner; in der digitalen Welt können dies Internet Service Provider, Suchmaschinenbetreiber, Telekommunikationsbetreiber oder auch Arbeitgeber sein.

Es ist nur schwer oder gar nicht möglich, einmal bekannt gewordene Daten wieder zu löschen, da dies die Kooperation der Datensammler – und ggf. auch derjenigen, die mittlerweile zusätzlich die Daten erhalten haben – erfordert.

3. Verkettung

Auch wenn Datensammlung, Verkettung und Auswertung teilweise kombiniert und in einer Hand durchgeführt werden, trennen wir hier die logischen Phasen, da der Datensammler und der *Verketter* nicht identisch sein müssen[17].

Die Verkettung der gesammelten Daten geschieht anhand eines Verkettungsalgorithmus, der je nach Anforderung anzupassen ist. Gegebenenfalls ist noch zwischen dem, der die Verkettung durchführt, und dem, der den Verkettungsalgorithmus dazu bereitstellt, zu unterscheiden, d.h., es gibt einen gesonderten *Verkettungsalgorithmus-Provider*. Das Verketten von Daten verfolgt üblicherweise einen vordefinierten Zweck. Auch die Sammlung von Daten kann schon zweckgesteuert sein; für Daten verarbeitende Stellen muss dies nach den Datenschutzgesetzen der Fall sein. Beispiele für Verkettungsmerkmale sind Adressen, aber es sind auch Verkettungen anhand von Inhaltsdaten oder Kontextinformationen möglich.

4. Auswertung

Die verketteten Daten werden in der Auswertungsphase interpretiert, wobei die *Auswerter* bestimmte Auswertungsalgorithmen – häufig statistische Modelle – verwendet werden. Auch diese Algorithmen werden unter Umständen von anderen zur Verfügung gestellt als denen, die sie zur Auswertung anwenden. Diese Anbieter kann man als *Auswertungsalgorithmus-Provider* oder *Modell-Provider* bezeichnen. Gerade wenn diese Modelle mit Wahrscheinlichkeiten arbeiten und/oder Prognosen liefern, besteht Ungewissheit ob der Korrektheit der Ergebnisse. Fehler lassen sich nicht völlig ausschließen. Nicht immer lässt sich der Grad der Ungewissheit, d.h. die Wahrscheinlichkeit (ggf. pro Ergebnisart), mit der der Algorithmus fehlerhafte Resultate erzeugt, beziffern.

Eine höhere Genauigkeit könnte in vielen Fällen erreicht werden, wenn statt der Auswertung durch statistische Modelle der Einzelfall detailliert untersucht würde. Dies ist allerdings ökonomisch teuer und in vielen Fällen auch invasiv für die Privatsphäre der einzelnen Betroffenen.

5. Generierung von Entscheidungen

Aufgrund der Auswertungsergebnisse in der vorherigen Phase werden von *Entscheidern* Entscheidungen getroffen, die für einzelne oder Gruppen von *Betroffenen* Folgen haben können. Sofern es sich um Entscheidungen handelt, die für den Betroffene eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen sie sich laut § 6a des Bundesdatenschutzgesetzes nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten stützen, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

Die Folgen solch ungenauer Entscheidungen können z.B. sein, dass der Betroffene unberechtigterweise keinen Kredit oder Handyvertrag erhält, dass sein Konto gesperrt oder sein Gehalt gepfändet wird, dass er einen Job nicht bekommt, dass seine Versicherungen teurer werden, dass er in einem Ermittlungsverfahren oder durch Rasterfahndung unter Verdacht gerät und weiter beobachtet oder

[17] Siehe auch die Ausführungen im Abschnitt 2.3.5 aus ökonomischer Perspektive, wonach die Übermittlung vom Datensammler zum Verketter und dann weiter zum Auswerter jeweils einen Geschäftszweig repräsentiert.

inhaftiert wird, dass er in einigen Ländern nicht einreisen darf oder auch, dass sein Ruf in einer Internet-Community oder im echten Leben leidet. Dabei kann es sein, dass sich bei einer genaueren Betrachtung die Entscheidung als falsch erweisen würde, z.B. weil es sich um eine Verwechslung handelt oder weil der Betroffene nur aufgrund der Zugehörigkeit zu einer Gruppe quasi in „Sippenhaft“ genommen wird und dadurch ungerechtfertigterweise mit betroffen wird.

2.2.4.2 Abhängigkeiten zwischen den Phasen

Im Phasenmodell der Informationsanreicherung erkennt man auf einen Blick, dass die Phasen aufeinander aufbauen. Eine fehlerhafte Entscheidung kann viele Ursachen haben, z.B.:

- Die gesammelten Daten als Grundlage für die Verkettung waren falsch.
- Die gesammelten Daten gehörten nicht zu der angenommenen Person, z.B. weil jemand anderes unter der Adresse aufgetreten ist.
- Beim Sammeln der Daten sind Fehler passiert.
- Beim Verketten wurden Fehler gemacht.
- Der Verkettungsalgorithmus oder dessen Implementierung wies Schwächen auf.
- Beim Auswerten wurden Fehler gemacht.
- Das Auswertungsmodell oder dessen Implementierung wies Schwächen auf.
- Bei der Entscheidung wurden nicht alle relevanten Informationen berücksichtigt.
- Bei der Übermittlung zwischen Datensammlern, Verkettern, Auswertern und Entscheidern kam es zu Fehlern.

In solchen Fällen kann es schwierig für einen Betroffenen einer Fehlentscheidung sein, sich dagegen zur Wehr zu setzen. Da der Datenfluss nicht immer gut nachvollziehbar und umfassend dokumentiert ist, ergeben sich – gerade wenn mehrere Akteure beteiligt waren – Schwierigkeiten beim Finden und Korrekturen von Fehlern.

Weiterhin zeigt das Phasenmodell, dass schon mit Festlegung von Adressen als mögliche Verkettungsmerkmale eine Designentscheidung gefällt wird. Beispielsweise wäre eine Verpflichtung zu E-Mail-Adressen im Schema „<vorname>.<nachname>@<provider>.de“ von daher kritisch zu sehen, weil sie einfach zu vielen anderen Dingen im Leben der Betroffenen verkettbar wären, weil sie dem Empfänger bereits den vollständigen Namen[18] enthüllen und weil sie sich von Außenstehenden erraten lassen, die dann unverlangte E-Mails (Spam) schicken können.

2.2.5 Privatsphärenrelevante Eigenschaften von Identitätsattributen

Verkettung kann sich auf die Privatsphäre von Menschen auswirken. Ein geeigneter Ausgangspunkt, um die Datenschutzeigenschaften von Identitätsattributen zu analysieren, ist das „Ich“. Biologisch und psychologisch, aber auch forensisch, ist von starkem Interesse, was einen Menschen prägt:

[18] Insbesondere Frauen lassen sich im Telefonbuch nicht mit dem vollständigen Vornamen eintragen, weil sie Belästigungen fürchten. Außerdem ermöglicht der Vorname häufig eine Einschätzung, wie alt der Betroffene ist.

- Ein Teil ist vorgegeben durch das Genom (die DNA), das natürlicherweise einen Link, also ein Verkettungsmerkmal, zum leiblichen Vater und zur leiblichen Mutter beinhaltet.[19]
- Der andere wesentliche Teil ergibt sich aus der Umgebung, z.B. wo man aufwächst und lebt, welche besonderen Erfahrungen man gemacht hat, welche Kontakte („Peers“) man hatte und hat.

Dies wird durch Abbildung 3 veranschaulicht.

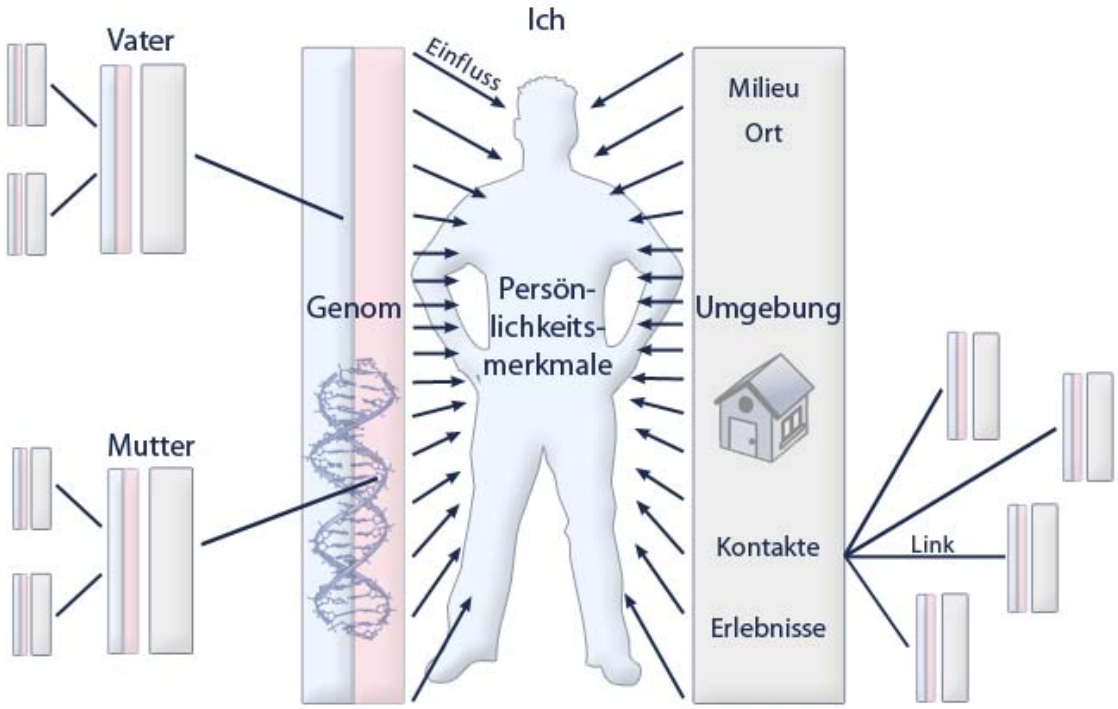


Abbildung 3: Genom und Umgebung als prägende Faktoren für das Ich

Während das Genom eines Menschen ein nicht-ablegbares Verkettungsmerkmal zu den Genomen der leiblichen Eltern und dann wiederum zu weiteren Blutsverwandten beinhaltet, sind die Links zur Umgebung häufig weniger fest[20] und nicht an einem einzigen Indikator wie der DNA festzumachen. Ein erheblicher Teil der menschlichen Persönlichkeit ist nicht ererbt und damit genetisch bereits codiert, sondern wird im Laufe der Entwicklung vom Kind zum Erwachsenen bis zum Lebensende erlernt. Bei der Prägung durch die Umgebung spielen insbesondere die Peers eines Menschen eine große Rolle, so dass für eine Beurteilung eines Individuums dessen soziales Netzwerk, d.h. eine Verkettung mit seinen Kontakten, umfangreiche Informationen mit hoher Aussagekraft liefern kann.

Wesentlich für die Privatsphäre sind die Persönlichkeitseigenschaften eines Menschen, also seine relativ zeitstabilen persönlichen Merkmale, insbesondere in Bezug auf sein Verhalten. „Relativ zeit-

[19] Eine erweiterte Betrachtungsweise stellt das „Metagenom“ dar, das zusätzlich zum Genom des Individuums sämtliche Erbinformationen der Mikroorganismen umfasst, die auf oder in ihm leben. Die Forschung zu diesen Mikroorganismen ist noch vergleichsweise jung. Es gibt aber bereits Hinweise, dass vor und bei der Geburt ein Teil der Mikroorganismen der Mutter zum Kind übertragen werden, so dass hier wiederum eine genetische Analyse eine Verkettungsmöglichkeit liefert.

[20] Beispielsweise kann man aus einem Ort wegziehen. Allerdings gibt es hier auch statische Komponenten wie z.B. der Geburtsort. Ähnliches gilt für Vergangenes im eigenen Leben, was nachträglich selbstverständlich nicht mehr änderbar ist und durchaus prägend sein könnte für das weitere Leben, z.B. die Information, dass man zu einem bestimmten Zeitpunkt an einem bestimmten Ort war (z.B. „Aufenthalt in Tschernobyl am 26. April 1986“).

stabil“ bedeutet, dass sich diese Merkmale bei wiederholter Messung nur unwesentlich und nur in einem gewissen vorhersagbaren Rahmen ändern dürfen. Änderungen sind projiziert auf einen längeren Zeitraum in begrenztem Maße möglich. Die Persönlichkeitseigenschaften können dazu dienen, das Verhalten eines Menschen in bestimmten Situationen vorherzusagen.

Privatsphärenrelevant ist insbesondere alles, was ein gezieltes Einwirken auf die Person, um deren Identitätsattribute es geht, ermöglicht oder fördert. Ein Einwirken-Können erfordert nicht zwangsläufig eine Identifikation des Betroffenen und schon gar nicht die Kenntnis des Namens[21]: Beispielsweise ist ein Anruf bei einem Unbekannten durchaus ein Eingriff in dessen Privatsphäre, denn er wird in seinem sonstigen Tun gestört. Das telekommunikative Herstellen der Verbindung stellt in diesem Fall die Verkettung dar: Der Anrufer kann die gewählte Telefonnummer mit der Stimme des Angerufenen in Beziehung setzen, er kann weiterhin durch bestimmte Aussagen auf ihn einwirken („Bei diesem Angebot sollten sie gleich zuschlagen!“ oder „Keine Polizei einschalten – ich beobachte Sie!“), und in vielen Fällen erfährt der Anrufer sogar den Namen des Angerufenen, wenn er sich entsprechend meldet.

Je mehr Informationen man über einen Menschen sammelt und verkettet, desto erfolgversprechender ist eine Manipulation, d.h. eine gezielte Beeinflussung: Bei Kenntnis von bestimmten Persönlichkeitseigenschaften wie den Interessen und den Dingen, auf die man emotional positiv reagiert, kann man gezielter zum Produktkauf animieren. Weiß man Bescheid über Finanzkraft und Suchtanfälligkeit für das Rauchen, kann es sich lohnen, den Betroffenen Gratis-Zigaretten zu schenken. Die Aussicht auf finanzielle Gewinne mag dabei ethische Grenzen in den Hintergrund treten lassen.

Im Folgenden werden Eigenschaften von Identitätsattributen danach sortiert, inwieweit sie für die Privatsphäre und mögliche Eingriffe relevant sind (siehe Tabelle 4). Oft hängt das Einstufen von Identitätsattributen gemäß diesen Eigenschaften von diversen Parametern ab, so dass sich nicht absolute Werte angeben lassen, die für alle Konstellationen Gültigkeit haben. Stattdessen sind in diesen Fällen auch die Zwischenwerte in dem Spektrum, das die im Folgenden genannten Eigenschaften aufspannen, zu betrachten.

[21] Siehe auch die Definition einer „Privacy“-Art von David J. Phillips, bei der nicht auf eine eindeutige Identifikation eines Individuums abgezielt wird, sondern auf die Segmentierung und Kategorisierung von Gruppen von Individuen [Phillips 2004]. Profiling- und Scoring-Methoden können dabei zum Einsatz kommen.

Eher weniger relevant für die Privatsphäre: keine gezielte Wirkung auf Person möglich	Eher potenziell privatsphäreninvasiv: gezielte Wirkung auf Person möglich
anonym	eindeutig identifizierend
nicht wiedererkennbar	wiedererkennbar
sich ändernd über die Zeit, ohne dass Dritte dies vorausberechnen können	stabil über die Zeit
leicht änderbar	nicht änderbar
weitergebbar / übertragbar	nicht weitergebbar / nicht übertragbar
flüchtig	langfristig gespeichert
nur einmal verwendet	häufig wiederverwendet
Authentizität unklar	authentisch
unbestätigt durch Dritte	bestätigt durch Dritte
Zugriff anderer darauf nicht möglich	Zugriff anderer darauf möglich
Zugriff anderer darauf transparent und kontrollierbar (durch aktive Willensentscheidung)	Zugriff anderer darauf nicht transparent und nicht kontrollierbar
keine Erreichbarkeit/Ansprechbarkeit ermöglichend	Erreichbarkeit/Ansprechbarkeit ermöglichend
als trivial oder unwichtig empfunden	zu den besonderen Datenkategorien gehörend oder als besonders sensibel empfunden
unauffällig / normal	auffällig / anormal
für einen oder wenige bzw. unwichtige Teile des eigenen Lebens relevant	für mehrere/wichtige Teile des eigenen Lebens relevant
keine zusätzlichen Informationen enthaltend	zusätzliche Informationen enthaltend, die bei Weitergabe nicht abtrennbar sind

Tabelle 4: Eigenschaften von Identitätsattributen

Beispielsweise sind biometrische Merkmale wie das Gesicht relativ stabil über die Zeit, nur eingeschränkt änderbar, nicht übertragbar, sie werden – in Zeiten der Speicherung eines biometrischen Passbildes auch digital im Passregister – langfristig gespeichert, häufig wiederverwendet, sind authentisch, man kann die Reisepassaushändigung als Bestätigung durch Dritte interpretieren, da das Gesicht meist unverhüllt ist, es können andere darauf zugreifen, was für den Betroffenen kaum kontrollierbar ist, und das Gesichtsbild enthält weitere Informationen wie z.B. das ungefähre Alter oder die Hautfarbe.

Ähnlich dicht am „Ich“ wie diese körperlichen Merkmale sind auch Persönlichkeitsmerkmale, die man schwer ändern kann – und wenn, dann ändert sich auch die Persönlichkeit.

Selbstbestimmte Identitätsmerkmale scheinen auf den ersten Blick weniger Einwirkung auf die Privatsphäre zu bedeuten als fremdbestimmte: Änderungen sind vielleicht gar nicht möglich sind oder erfordern ggf. die Mitwirkung Dritter. Dies bedeutet zumindest einen höheren Aufwand. Außerdem kann der Betroffene für den Fall, dass die fremdbestimmende Stelle das Identitätsmerkmal kennt, Zugriffe darauf (z.B. durch eine Weitergabe) in der Regel nicht kontrollieren. Allerdings enthüllen selbstbestimmte Identitätsmerkmale häufig zusätzliche Informationen über die Persönlichkeit des Betroffenen. Dies zeigt sich beispielsweise bei der Wahl von Pseudonymen, die sich am eigenen Namen oder an Vorbildern orientieren, die das Geburtsjahr enthalten. Dazu kommt, dass Nutzer solche selbstgewählten Pseudonyme gern übergreifend für mehrere Lebensbereiche verwenden, so dass weitere Informationen verkettbar werden.

2.3 Grundlagen verschiedener fachlicher Disziplinen

2.3.1 Historische Grundlagen

2.3.1.1 Einleitung

Ein elementares Merkmal zur Unterscheidung von Personen ist der Name. Dieser stellt zudem ein wesentliches Element der Identität eines Menschen dar und kann Auskunft über seine Abstammung geben. Aus historischer Sicht ist vor allem die Herkunft, Entwicklung und Bedeutung von Namen interessant, weshalb hierauf in diesem Kapitel näher eingegangen wird.

Neben dem Namen ist auch die Zugehörigkeit zu einer oder mehreren sozialen Gruppe(n) ein wichtiger Bestandteil der Identität einer Person. Im Hinblick auf digitale Identitäten gewinnen insoweit Internet-Communities zunehmend an Bedeutung. Aus historischer Sicht sind hingegen vor allem die sozialen Gebilde Familie, Sippe und Stamm von Interesse.

Gerade der Staat besteht in vielen Fällen darauf, dass der Bürger ihm gegenüber seine Identität offenbart. Dabei erfolgt eine Identifizierung herkömmlicherweise mit Hilfe eines Identitätsdokuments, weshalb in diesem Kapitel auch auf die historische Entwicklung solcher Dokumente eingegangen wird: Diese reicht von den Passierscheinen des Mittelalters bis zu den Personalausweisen und Reisepässen der Neuzeit.

Historisch betrachtet wurden zielgerichtete Verkettungen von Daten zunächst überwiegend von Staat Kirche vorgenommen. Neben Volkszählungen wurden insoweit schon früh auch Register, also systematische Sammlungen von Informationen über eine Gruppe von Personen oder Objekten, verwendet. Deshalb wird nachfolgend ein Abriss zu der historischen Entwicklung von Registern gegeben, der von dem Personenerfassungssystem der Kanzlei des Staufers Friedrich II. über die ab dem 16. Jahrhundert geführten Kirchenbücher bis zu den modernen Melderegistern reicht.

2.3.1.2 Herkunft, Entwicklung und Bedeutung von Namen

Der Name (lat.: nomen, griech.: onoma) einer Person bestimmt ein Einzelwesen in Unterscheidung von anderen und ist damit ein unmittelbares Identifizierungsmerkmal.

Der heutige Familienname (Nachname, Zuname) dient als Ergänzung zum Vornamen der exakteren Unterscheidbarkeit von Personen. Im Deutschen nach dem Vornamen platziert, bezeichnet er die Zugehörigkeit zu einer Familie.

Die Angehörigen verschiedener germanischer Stämme führten in der Regel nur einen Namen, wobei in Einzelfällen der Name des Vaters oder die Bezeichnung individueller Eigenschaften mit angegeben wurde. Ab dem 12. Jahrhundert wurden zunehmend zweinamige Bezeichnungen gebräuchlich, wobei eher von Beinamen auszugehen ist, da die Merkmale heutiger Familiennamen – wie Erblichkeit und Festigkeit – für diese Zeit bislang nicht nachgewiesen werden konnten. In den romanischen Ländern setzte diese Entwicklung früher ein – so etwa in Venedig bereits im 9. Jahrhundert in Florenz und Verona im 10. und in Südfrankreich im 11. Jahrhundert.

Als Beinamen zur näheren Personenkennzeichnung finden Verwendung:

- Verwandtschaftsangaben, z.B.
  - Vaternamen (Patronym) und
  - Mutternamen (Matronym);
- Amts- und Berufsbezeichnungen;
- Herkunftsnamen (Toponyme, insbesondere hinsichtlich Land, Ort, Haus) oder
- Übernamen (Eigenschaften, Gewohnheiten).

Als Gründe für das Aufkommen von Beinamen werden genannt:

- kommunikative Gründe;
- wirtschaftliche Interessen oder
- juristische Gesichtspunkte.

Eine unmissverständliche Identifizierung des Einzelnen war in den zunehmend größer werdenden Gemeinwesen nicht mehr gewährleistet Mit der Erblichkeit der Lehen ab 1037 war (vor allem) dem Adel daran gelegen, dass der Besitz „in der Familie“ blieb. Durch den Ausbau der Verwaltung und die Zunahme der Schriftlichkeit im 13. und 14. Jahrhundert mussten Registereinträge und Vertragsabschlüsse personell eindeutig zuordenbar sein.

Obwohl sich bis zum 15./16. Jahrhundert die Zweinamigkeit weitgehend durchgesetzt hatte, galt noch lange der Rufname als der eigentliche Name, der auch in diversen Registern geführt wurde. Erst im Laufe des 18. Jahrhunderts wurde die Verbindlichkeit und Beständigkeit des Familiennamens durchgesetzt – in Mitteleuropa abschließend mit dem napoleonischen Dekret von 1811. Veränderungen waren noch in Ausnahmefällen möglich: durch Eindeutschung fremd klingender Namen, Adoption, Legitimation unehelicher Kinder, Eheschließung, Ehescheidung, Nobilitierung, Konfessionswechsel, Namensverleihung für Findelkinder, Doppelnamen bei allzu häufigen Namen (wie z.B. Müller-Lüdenscheid), Künstlernamen und Ordensnamen.

In Deutschland kam mit der Einführung des Standesamtes 1874 der jahrhundertealte Prozesse der Ausbildung erblicher, fester Familiennamen zu einem Abschluss: Die Schreibweise wurde festgelegt, jegliche Familiennamenänderung der behördlichen Genehmigung unterzogen.

Die etymologische Herkunft soll hier angesichts eines Bestands von derzeit ca. ½ Million Familiennamen deutscher Herkunft, deren Formenvielfalt nicht zuletzt mit den gängigen Schreibvarianten, früheren Übermittlungsfehlern, unklarer Orthographie u.Ä. zusammenhängt, nicht näher untersucht werden.

Als Beispiele für Familiennamen, in denen eine genealogische Kontinuität sichtbar wird, können die in norddeutschen und skandinavischen Ländern gebräuchlichen patronymischen Namen auf der Endung „-sen“ („-son“) genannt werden. Auf Island und den Färöern besteht der zweite Name aus dem Namen des Vaters, erweitert um „-son“ (Jungen) und „-dóttir“ (Mädchen).

Die Benennung nach der Mutter war in früheren Zeiten nur bei unehelichen Geburten üblich. Heute können die Ehegatten den Geburtsnamen oder den zur Zeit der Eheschließung geführten Namen der Frau oder des Mannes zum Ehenamen bestimmen[22]. Zudem kann ein Ehegatte, dessen Name nicht Ehename wird, dem Ehenamen seinen Geburtsnamen oder den zur Zeit der Eheschließung geführten Namen voranstellen oder anfügen[23].

In den iberischen Ländern erhalten die Kinder als Familiennamen jeweils einen Teil des väterlichen, wie auch des mütterlichen Nachnamens.

In Schottland drückt die Vorsilbe Mac die Zugehörigkeit zu einem bestimmten Clan (von gälisch: Clan = Abkömmlinge) aus, dessen Mitglieder sich als Nachfahren eines (auch mystischen) Ahnen empfinden, jedoch nicht direkt verwandt sein müssen. In Irland wird der gleiche Zusammenhang mit dem vorgesetzten O’ bezeichnet.

[22] § 1355 Abs. 2 BGB.

[23] § 1355 Abs. 4 BGB. Dies ist allerdings dann nicht möglich, wenn bereits der Ehename aus mehreren Namen besteht. Auch kann zum Ehenamen nur ein Name hinzugefügt werden: Besteht also der – nicht zum Ehenamen werdende – Name eines Ehegatten aus mehreren Namen, so kann nur einer dieser Namen dem Ehenamen hinzugefügt werden.

2.3.1.3 Familie, Sippe, Stamm – historische Vorläufer der Internet-Communities

Historische Vorläufer der heutigen Internet-Communities sind unterschiedliche Arten von Gemeinschaften wie Familie, Sippe und Stamm, denen eine Person angehören kann.[24]

2.3.1.3.1 Begriff der Gemeinschaft („Community“)

Gemeinschaft[25] bezeichnet eine Einheit von Individuen (Gruppe), die in einer Beziehung zueinander stehen. Zumeist liegt eine gemeinsame Tätigkeit, ein Anliegen oder Ziel zu Grunde, wodurch ein Zusammengehörigkeitsgefühl („wir“) produziert wird, das auch immer eine Trennungslinie gegenüber den „anderen“ zieht.

Im Deutschen sind in diesem Zusammenhang vor allem die Begriffe mit dem Suffix „-schaft“ zu betrachten:

- Verwandtschaft;
- Nachbarschaft;
- Freundschaft;
- Körperschaft;
- Burschenschaft;
- Mannschaft oder
- Wissenschaft etc.

Lebensgemeinschaften (z.B. Ehe oder Orden) gehören ebenso dazu wie Zwangsgemeinschaften, Schicksalsgemeinschaften, wirtschaftliche Gemeinschaften (Interessenvertretungen, Kooperativen), religiöse Gemeinschaften oder wissenschaftliche Gemeinschaften.

Diese Gemeinschaften sind zu unterscheiden nach:

- Inhalten (Tätigkeiten), die die Gemeinschaft konstituieren, und
- Formen (Instrumente, Technologien), die diese Inhalte kommunizieren.

2.3.1.3.2 Historische Vorläufer der heutigen Internet-Communities

Der 1985 in Sausalito (USA) gegründete netzbasierte Debattierclub „The Well“ (The Whole Earth 'Lectronic Link)[26] hat einen Vorläufer in der „Res publica literaria“ (der Gelehrtenrepublik). Dieser Begriff war bis ins 18. Jahrhundert hinein gebräuchlich und bezeichnete die Verbindung des internationalen (europäischen) Wissenschaftsbetriebs. Dazu gehörten wissenschaftlich Publizierende und alle, die im wissenschaftlichen Austausch miteinander standen: Universitätsprofessoren, Bibliothekare, Archivare, Historiker in öffentlichen Positionen, Theologen in kirchlichen Ämtern und Privatgelehrte. Gesammelt, kanalisiert und den jeweiligen Obrigkeiten zur Verfügung gestellt wurde das Wissen durch die „Akademien der Wissenschaft“ in den einzelnen Ländern – gewissermaßen die Knotenpunkte im Netz.

In der Vermittlung von Wissen sollten weder Standes- noch Religions- noch Nationalitätsvorbehalte gelten – insofern existierte also ein demokratisches Gemeinwesen in Zeiten allgegenwärtiger Monarchie.

---

[24] Natürlich gibt es in der Moderne nicht nur Internet-Communities, sondern weiterhin verschiedene Sozialformen, die nebeneinander existieren.

[25] Die Endung „-schaft“ kommt vom althochdeutschen „Scaf“, was soviel heißt wie Beschaffenheit, und aus derselben indogermanischen Wurzel wie „schaffen“.

[26] „Well“ ist das englische Wort für „Brunnen“ – dieser Begriff wurde nicht ganz zufällig gewählt, da der Brunnen für dörfliche Gemeinschaften gleichsam Wasserquelle und Treffpunkt für einen Informationsaustausch darstellte.

Das gängige Medium war die kontinuierliche und zügige briefliche Korrespondenz – so konnte der Pathologe G. B. Morgagni aus Bologna bereits im 16. Jahrhundert regelmäßige wöchentliche Briefe mit seinem Kollegen in Leyden wechseln. Umfangreiche Adressensammlungen erlaubten es bei Reisen in fremde Städte/Länder, bei Fachkollegen vorzusprechen und den schriftlichen Austausch zu personalisieren. In der üppigen Reisetagebuchliteratur des 15.-18. Jahrhunderts finden sich denn auch aufschlussreiche persönliche Bemerkungen über private Eigenschaften und Lebensumstände der hochverehrten Kollegen. Mit der zweiten Hälfte des 17. Jahrhunderts kam das literarische Journal als zentrales Kommunikationsmedium dazu: Die allgemeine Verbreitung von Meinungen und Informationen an einen unübersehbaren Adressatenkreis. Persönlich gezeichnete Kritiken und Rezensionen ermöglichten weiterhin den direkten Austausch – insoweit bestand also auch hier eine Art von Gemeinschaft im oben erläuterten Sinne.

Waren „Literatur“ und „Gelehrsamkeit“ bis ins späte 18. Jahrhundert synonym verwandt worden, wurde der Begriff „Res publica literaria“ im Verlauf des 19. Jahrhunderts ungebräuchlich, da die Literatur als Bereich der künstlerischen Freiheit von der Begrifflichkeit der Fachwissenschaften getrennt wurde.

Heutzutage bezeichnet eher die englische Bezeichnung „Scientific Community“ die Tatsache eigener Kommunikation(swege) und Kontakte unter Wissenschaftlern.

2.3.1.3.3 Kommunikationsmedien von Gemeinschaften

Kommunikationsmedien von Gemeinschaften sind insbesondere:

- mündliche Überlieferungen (fahrende Sänger, Märchen und Sagen),
- schriftliche Mitteilungen wie
  - religiöse Überlieferungen (heilige Schriften),
  - Rechtskodizes als Verhaltens- und Verfahrensregelung,
  - (wissenschaftliche /literarische) Druckerzeugnisse zur massenhaften Meinungsbildung,
  - Briefe (an mehrere Adressaten: z.B. Apostelbriefe, Rundbriefe, Lehrbriefe, Reiseberichte; an einzelne Adressaten: private / geschäftliche Briefe),
- persönliche Kontakte (individueller Austausch und Beurteilung),
- Tradierung äußerer Merkmale (Kleidung, Haartracht, Standesabzeichen)

In der frühen (europäischen) Zeit erfolgte die Überlieferung und Kommunikation überwiegend mündlich: So zogen etwa in Skandinavien ab dem 10. Jahrhundert die Skalden (fahrende „Sänger“, die allerdings nicht sangen, sondern in Reimform rezitierten) von Hof zu Hof. Sie gaben in einer Mischung aus überlieferten und improvisierten Vorträgen genealogische Gedichte (z.B. Ynglingatal[27]) zum Besten, mit denen sich die Menschen die Zeit vertrieben und Neuigkeiten sowie Wissenswertes über ihre Geschichte und Vorfahren erfuhren.

Die Trobadore und Minnesänger des Mittelalters trugen sodann vorwiegend die Kunde von schönen Frauen und damit verbundenen Liebesangelegenheiten weiter. Die Bänkelsänger, die seit dem 17. Jahrhundert (bis in die 1930er Jahre) über Land zogen, erfüllten die Funktion von Radio, Fernseher und Kino, indem sie Nachrichten und Meinungen mündlich überlieferten: Mord, Liebe, Katastrophen und aufregende politische Ereignisse wurden (meist mit passender Schlussfolgerung – der Moritat) dem Publikum zur Kenntnis gebracht.

Die schriftliche Überlieferung war bis zur Erfindung bzw. Etablierung des Buchdrucks Sache der Klosterkopisten, die sakrale Überlieferungen und Texte ausgewählter antiker Autoritäten handschriftlich für einen kleinen, schriftkundigen Benutzerkreis herstellten.

Die Erfindung des mechanischen Buchdrucks mittels beweglicher Metall-Lettern durch Johann Gensfleisch genannt Gutenberg, Mitte des 15. Jahrhunderts, bezeichnet einen Meilenstein in der

[27] Nach einer Legende war Ynglingatal der Stammbaum der Herrscher des Königsgeschlechts der Ynglinger. Diese Legende war Vorbild für das Kapitel „Ynglinga saga“ in Snorri Sturlusons Werk Heimskringla.

Geschichte der Informationsweitergabe durch Sprache (Oralität) und Schrift (Literalität). Sie ermöglichte die exakte massenhafte Reproduktion von (Wissens-)Inhalten, die allgemeine Alphabetisierung, ja gar Anpassung des menschlichen Denkens an die Schriftform (Entwicklung von linearem und kausalem Denken).

Ein weiteres wichtiges Medium der (nonverbalen) Kommunikation ist die Kleidung. Dieser kommt neben einer Schutz immer auch eine Markierungsfunktion zu: Als Kommunikationsmittel bezeichnet sie die Mitglieder einer Gruppe (und damit oft deren soziale Stellung) und lässt sich differenzieren nach:

- Nation (Stamm): z.B. Burnus, Toga, Tunika
- Religion: Kopftuch, Burka, Kippa, Mönchshabit
- Amt/Beruf: Uniform, Dienstkleidung
- Verein: Tracht, Funktionskleidung
- Besonderer Anlass: Hochzeits-, Trauerkleidung

Abschließend sei der Blick noch kurz in die Gegenwart gerichtet: Bei einer vor wenigen Jahren durchgeführten Umfrage der Zeitschrift „Die Zeit“ erklärte die Mehrheit der Befragten, dass die persönliche Begegnung mit ihrem vielfältigen direkten (mündlichen) Austausch nach wie vor ihr Kommunikationsfavorit sei[28]. Auf dem nächsten Platz folgte das Telefonieren mit der Möglichkeit von Rede und Gegenrede (ebenfalls mündlich). Die positiven Seiten von Handytelefonaten – jederzeitige Erreichbarkeit, Beschleunigung aller Vorgänge, eingeforderte unmittelbare Reaktion – werden allerdings ebenso oft als deren gravierendste Nachteile bewertet (Ähnliches gilt für die Kommunikation via SMS). Postkarten, Telegramm und Fax hingegen verlieren als „altertümliche“ Kommunikationsmittel zusehends an Bedeutung. Briefe werden nach wie vor gerne erhalten, aber – nicht zuletzt aus Zeitmangel – ungern geschrieben.

2.3.1.4 Historischer Abriss zu Registern und Identitätsdokumenten

2.3.1.4.1 Einleitung

„Überprüfen Sie das bitte!“ Die Tatortkommissarin, die ihren Assistenten mit dieser Aufforderung und dem Ausweis des Verdächtigten zur Online-Abfrage in den Einsatzwagen schickt, will mehrfache Gewissheit. Ist der Betreffende der, der er zu sein vorgibt, ist sein Ausweis „echt“, d.h. amtlich registriert, und gibt es vielleicht noch weitere Einträge zu seiner Person?

Bereits in früheren Zeiten mussten sich Menschen in bestimmten Situationen ausweisen, d.h. beweisen, dass sie auch tatsächlich derjenige waren, der sie dem Augenschein und der eigenen Versicherung nach waren. Neben der persönlichen Beteuerung von anwesenden Bekannten, die über die Identität der fraglichen Person Zeugnis ablegen konnten, entstanden im Laufe der Zeit verschiedene Formen schriftlicher Ausweise.

Zum Beweis der Echtheit eines Ausweises wurden und werden Personenregister als Glaubwürdigkeitsreferenz geführt, deren wichtigste die Melderegister sind. Diese dienen Staat und Wirtschaft als Informationsquelle und ermöglichen umfassende Verkettungen digitaler Inhalte.

Nachfolgend wird ein Überblick über die historische Entwicklung von staatlichen Identitätsdokumenten und Registern gegeben.

[28] Ulrich Stock, „Die Hitparade der Kommunikationsformen“ in Die Zeit, Heft 32/2001, abrufbar unter http://www.zeit.de/2001/32/liebe_hass.xml (letzter Zugriff im Oktober 2007).

2.3.1.4.2 Historischer Abriss zu staatlichen Registern und Identitätsdokumenten

In begrenzten Augenschein-Gesellschaften wie der griechischen Polis waren keine gesonderten Identifizierungsmaßnahmen vonnöten, da jeder Bürger als Person und in seiner spezifischen gesellschaftlichen Funktion persönlich bekannt war[29].

Im unübersehbaren Römischen Reich griff die Obrigkeit gelegentlich zum Mittel der Volkszählung, wie es die christliche Überlieferung in der Weihnachtsgeschichte zu berichten weiß, als Kaiser Augustus „den Befehl gab, alle Bewohner des Reiches in Steuerlisten einzutragen. Da ging jeder in seine Stadt, um sich eintragen zu lassen“ (Lukas, 2,1). Angaben über den Untertanenbestand waren für die Machthaber wichtig zur Berechnung einzutreibender Steuern sowie potenzieller Legionäre und Sklaven. Sie boten allerdings keine Grundlage für eine individuelle Identifizierung.

Die Kanzlei des reformerischen Staufers Friedrich II. führte im 13. Jahrhundert in dem kameralistisch organisierten Beamtenstaat in Sizilien erstmals ein schriftliches System der Personenerfassung ein, das ein Prinzip späterer Einwohnermeldeämter vorwegnahm: Das amtlich beglaubigte Register als verlässliche Grundlage, anhand derer Aussagen zu einzelnen Personen getroffen werden konnten.

Diese Idee setzte sich im europäischen Mittelalter zunächst nicht durch. Schriftliche Bestätigungen der Person gab es für vermögende Bürger, Adelige und Verbrecher. Höhergestellte Personen benötigten beispielsweise Ausweise, um sicher von A nach B zu gelangen. Persönlich ausgestellte Pass(ier)dokumente, Visa und Geleitschreiben ermöglichten es, die Risiken des Reisens zu minimieren. Es handelte sich bei ihnen um Schutzbriefe, in denen eine mächtige Referenzperson sich für die Unbedenklichkeit und Schutzwürdigkeit des namentlich Genannten verbürgte.

Steckbriefe zur Fahndung nach Verbrechern konnten nach der Erfindung des Buchdrucks vielfältig publiziert werden und so einem großen Personenkreis ein wortreiches „Signalement“ des Gesuchten zur Kenntnis bringen.

Als Beispiel einer massenhaften Registrierung von Personen werden die Namenslisten von Auswanderern genannt, die Ende des 15. Jahrhunderts aus portugiesischen Häfen in die „Neue Welt“ aufbrechen wollten. Dabei sollten bestimmte Gruppen als Kolonialisten ausgeschlossen bleiben. Es handelte sich hierbei allerdings um ein störanfälliges System, da die Authentizität der angegebenen Namen nicht gewährleistet war.

Die katholische Kirche, die sich nach den Wirren der Reformation ihrer Gläubigenbestände versichern musste, entschied 1563 beim Konzil von Trient, hinfort in allen Pfarreien Aufzeichnungen über die Pfarrkinder zu führen. Im 18. Jahrhundert verpflichtete Kaiser Josef II. die Pfarrherrn aller Konfessionen, für staatliche Zwecke Zweitschriften über die Taufen von Neugeborenen, Eheschließungen und Beerdigungen anzufertigen. Diese Angaben wurden wohl als die wichtigsten Merkmale einer Person angesehen, machten sie doch aus christlicher Sicht die wahre „identitas“ eines Menschen aus: Durch die Taufe in die Gemeinschaft der Gläubigen aufgenommen, vor Gott zu Mann und Frau erklärt, mit dem Segen der Kirche beerdigt: Nur so kann ein Individuum, d.h. der nicht teilbare, vollständige – auch nach Krankheit, Verwundung und Tod wiederhergestellte – Körper beim Jüngsten Gericht bestehen und in die ewige Seligkeit eingehen.

Diese Kirchenbücher stellten so auch für die jeweiligen Landesherren lange die einzigen verlässlichen Angaben über die eigenen Untertanen zur Verfügung: Anzahl, Geschlecht, Alter, Wohnort und gelegentlich Beruf. Damit konnten diese Informationen zur Person, die von einer registerführenden Stelle an die nächste weitergegeben wurden, zu weiteren obrigkeitlichen Zwecken Verwendung finden: Im Mittelpunkt des Interesses standen insoweit die Verwendung von Angaben zu Zwecken der Besteuerung, der Aushebung von Rekruten und der Armenversorgung.

Die „Policey“ als allgemeine obrigkeitliche Verwaltungsinstanz führte im 16. Jahrhundert Personenregistrierungen im Zusammenhang mit der Armenfürsorge ein. Die Erfassung, Überwachung und Versorgung der massenhaft umherziehenden Vaganten – Bettler, Krüppel, Dirnen, Kriegsversehrte,

[29] Zu Zeiten Solons ging man davon aus, dass eine Demokratie von mehr als 20.000 Menschen nicht bestehen könne, da eben diese Bedingungen der persönlichen Bekanntschaft, des Vertrauens und der hierarchischen Eingebundenheit bei einer größeren Anzahl von Menschen nicht mehr gegeben seien.

Aussätzige, Schausteller – wurde durch schriftliche Fixierung der Personen zu berechenbaren Größen.

Amtliche Registrierung betraf in der Regel Arme, Verdächtige oder sonstige Inkriminierte. Zum Nachweis des „Heimatrechts“ wurden gemeindliche Personenregister geführt, die eine Voraussetzung für die Armenfürsorge bildeten. Lokal ansässige Bedürftige hatten einen anderen Anspruch auf Versorgung als umherwandernde.

Der Höhepunkt der französischen Revolution bescherte mit der Einführung des „Code civil“ am 20. September 1792 die Geburtsstunde der genuinen, säkularen Personenerfassung und damit der modernen Staatsbürgerschaft. Nicht mehr kirchliche, sondern nur mehr staatliche Instanzen sollten in Zukunft alle Personen ihres Hoheitsgebiets direkt administrativ erfassen und damit identifizieren können. Als ausgewiesener Staatsbürger galt nun (nur noch) eine natürliche Person, die über einen papiernen Ausweis verfügte zu der zusätzlich auch noch ein mit dem Ausweis übereinstimmender Eintrag in einem amtlichen Register vorlag. Mit diesem „Ausweis“ des papiernen Ausweises konnte dann dessen Echtheit nachgewiesen werden.

Die wenige Jahre zuvor im revolutionären Freiheitsrausch begeistert abgeschaffte Ausweispflicht war in der Zwischenzeit aufgrund der unruhigen politischen Verhältnisse wieder eingeführt worden. Ein Dilemma, das sich durch das gesamte 19. Jahrhunderts zieht: Auf der einen Seite die zunehmende Liberalisierung der gesellschaftlichen und wirtschaftlichen Bedingungen, die eine ungestörte Freizügigkeit ohne restriktive Ausweisregelungen erforderte, auf der anderen Seite die in regelmäßigen Abständen – insbesondere in tatsächlichen oder vermeintlichen Krisenzeiten – wiederkehrenden obrigkeitlichen Bestrebungen zur Verstärkung der Erfassung und damit der Kontrolle von Staatsvolk und Fremden.

Mit dem Übergang vom absolutistischen Staat in den bürgerlichen Rechtsstaat des 19. Jahrhunderts änderte sich auch die Beziehung zwischen Staat und Staatsbürger. Diese wurde unter anderem durch dessen Identitätsausweis, den Pass, geregelt, der ihm neben Kontrolle auch einen gewissen Schutz des Staates eintrug. Für den Staatsangehörigen berechtigt er nach dem Recht des ausstellenden Staates zum grenzüberschreitenden Reisen und im Grundsatz auch zur Rückkehr ins eigene Land.

Das Allgemeine „Pass-Edikt für die Preußische Monarchie“ von 1817 und das nachfolgende Preußische „Gesetz über die Aufnahme neu anziehender Personen“ von 1842 verlangte die namentliche Meldepflicht aller durchreisenden Personen, wie es die Polizeiliche Aufsicht über Reisende und Fremde in Gasthöfen und Herbergen vorsah.

Für die im Norddeutschen Bund zusammengeschlossenen Länder galt das 1867 verabschiedete „Gesetz über die Freizügigkeit“, das seine Gültigkeit bis zum Ende der Weimarer Reichsverfassung behielt.

Zum Ende des 18. Jahrhunderts wurden in Städten die ersten Adressbücher oder Adresskalender aufgelegt. Ihr Anspruch war es, ein möglichst exaktes Verzeichnis aller Einwohner nebst ihres Wohnhauses und dessen Beschaffenheit sowie ihres Familienstandes und Berufs zu erstellen. Topographische, statistische und administrative Verhältnisse der jeweiligen Stadt wurden beigefügt. Es ist allerdings eher unwahrscheinlich, dass diese Register von Provinzial- oder Staatsregierungen zu einem Gesamtbestand zusammengeführt wurden[30].

Daneben wurden Spezialverzeichnisse verschiedener Gruppen veröffentlicht: So wurde etwa die Angehörigen eines Staatsapparates wurden im jährlich aufgelegten Staatshandbuch aufgelistet. Nach dem Vorbild des Pariser „Almanach royal“ von 1679 fanden sich in solchen Handbüchern Angaben über den Souverän und seinen Hof sowie ein Namensverzeichnis aller Staatsbeamten und ihrer Behörden. Das umfangreiche „Handbuch für das Deutsche Reich“ von 1893 enthielt darüber hinaus den Nachweis der Befugnisse der Staatsdiener und der von diesen zu erbringenden Leistungen. Das englische Pendant war das „Statesman’s Yearbook“, das seit 1864 in London erschien.

Mitglieder von Adelshäusern fanden ihr adäquates Personenregister im seit 1764 veröffentlichten „Gothaischen Genealogischen Hofkalender nebst diplomatisch-statistischem Jahrbuch“ (dem bis auf

[30] Zumindest ist nicht bekannt, dass ein solcher Bestand in Deutschland existiert hätte.

den heutigen Tag gepflegten „Gotha“), das „für den internationalen Verkehr wertvolle Nachrichten“ über Land und vor allem Leute enthielt.

Mit zunehmender wirtschaftlicher Prosperität führten im 19. Jahrhundert ganze Berufs-, Erwerbs- und Industriezweige spezifische (nichtamtliche) Verzeichnisse. Das „Adressbuch des deutschen Buchhandels und der verwandten Geschäftszweige“ diente ebenso der schnellen Information und Kommunikation wie das „Reichsadressbuch deutscher Industrie- und Handelsfirmen“, das 1892 in zwei Bänden erschien.

Anders als heute wurden im 19. Jahrhundert nie Firmen, sondern immer einzelne Personen in bestimmten Positionen adressiert[31].

Im Hamburger „Gesetz über das Meldewesen“ von 1929, das 1933 von Preußen übernommen wurde, wurde erstmals eine Mitteilungspflicht der Meldebehörden gegenüber einer Reihe von anderen Behörden und Stellen geschaffen. Persönliche Daten durften insoweit zu verschiedenen weiteren Zwecken verwandt werden.

War bis dato das Meldewesen in Deutschland Länderangelegenheit gewesen, so wurde 1938 vom Reichsinnenminister erstmals ein reichseinheitliches Meldesystem vorgestellt. Nationalsozialistisches Gedankengut, das die Kontrolle der Bürger auf alle Lebensbereiche ausdehnte, forderte verschärfte Meldepflichten für alle Beherbergungs-, Aufenthalts- und Versammlungsorte. Der Datenaustausch zwischen einzelnen Meldebehörden wurde in Form der Rückmeldung verbindlich eingeführt. Die Melderegister sollten damit als zentrale Informationsstellen für staatliche, kommunale und polizeiliche Aufgaben fungieren, aber auch für Parteizwecke nutzbar gemacht werden. Bei „auffälligen“ Personenmerkmalen, nicht genehmer Rassezugehörigkeit, erbbiologisch interessanten Daten, Aus- oder Rückwanderung von Personen wurde routinemäßig die Gestapo informiert. Der Austausch von Personendaten bewirkte in diesem Zusammenhang größtmöglichen Schaden für die betroffene Person.

Vor der Einführung des Personalausweises galt in Deutschland die Kennkarte als amtlicher Legitimationsnachweis. Ihr Besitz war jedoch nicht allgemein verpflichtend, ab Juli 1938 war das Mitführen der gebührenpflichtigen Karte dann aber für Juden obligatorisch. Im Format DIN A6 aus grauem, leinenverstärkten Papier enthielten die Karten ein Passbild des Inhabers, seine persönlichen Meldedaten, den Fingerabdruck und ein eingestempeltes großes „J“.

Die im April 1939 erlassene Verordnung über die Einrichtung einer „Volkskartei“ wurde noch bis 1944 weiter ausgebaut, dann unter den Bedingungen des totalen Kriegs fallengelassen. Ziel war die möglichst vollständige Erfassung aller Daten der gesamten Bevölkerung in allen Lebensbereichen.

Die bereits erwähnten Kirchenbücher wurden in der NS-Zeit ebenfalls zu politischen Zwecken genutzt: Mit ihrer Hilfe wurde der Nachweis der „arischen“ Abstammung geführt.

Geburt, Heirat und Tod werden seit 1876 in Deutschland nicht nur in den Kirchenbüchern dokumentiert, sonder auch staatlicherseits in den sog. Personenstandsbüchern beurkundet. Das Personenstandsgesetz (PStG) von 1937 regelt die formalen Voraussetzungen zur Begründung und Änderung des Personenstandes. Registriert werden neben Geburten, Heiraten und Sterbefällen auch verschiedene andere Veränderungen des Personenstandes wie Scheidungen, Kirchenaustritte und Geschlechtsumwandlungen. Auch wenn es hier um historische Grundlagen geht, sei in diesem Zusammenhang noch ein Blick in die Zukunft gestattet: An die Stelle der herkömmlichen Personenstandsbücher werden in Deutschland während einer Übergangszeit vom 1. Januar 2009 bis zum 31. Dezember 2013 elektronische Personenstandsregister (Geburts-, Ehe-, Lebenspartnerschafts- und Sterberegister) treten[32,33].

[31] Dazu passend konnten komplette Sätze oder nach gewissen Kriterien ausgewählte Klebeadressen für den Postversand bestellt werden.

[32] Die Rechtsgrundlage hierfür findet sich im Personenstandsrechtsreformgesetz (PStRG) vom 19.02.2007.

[33] Folgende Literatur hat Eingang in diesen Abschnitt gefunden: [Kohlheim 2005], [Moos 2004], [Caplan 2001], [Fahrmeier 2000], [Gosewinkel 2001], [Groebner 2004], [Medert/Süßmuth 2005] und [Wesel 2006].

2.3.2 Soziologische Grundlagen

2.3.2.1 Einleitung

Der institutionalisierte Datenschutz beobachtet professionell andere professionelle Beobachter. Datenschutz macht deshalb die Organisation von Beobachtungen zum Thema. In der Datenschutz-Kommunikation wird „das Wie des Beobachtens“ praktisch-reflexiv. Dies geschieht nicht als folgenlose erkenntnistheoretische Übung, sondern durch praktische Beobachtung der Kommunikation von Organisationen mit deren Klientel. Beurteilt wird die Fairness von Kommunikationsbeziehungen. Konkret geht es darum, wie staatliche Behörden, private Firmen und Hilfe leistende Praxen ihre externe Klientel (Bürger, Kunden oder Verbraucher, Patienten) und ihre internen Mitglieder (Mitarbeiter, Mitglieder) so einbinden, dass die dadurch erfolgenden Einschränkungen der Autonomie der Betroffenen transparent, dadurch zustimmungs- oder ablehnungsfähig und reversibel sind und deren Fairness sowohl für die Beteiligten als auch berechtigte Beobachter abschätzbar ist.

Die datenschutztheoretischen Überlegungen zur Organisation von Beobachtungstechniken basieren auf dem Begriff der Verkettbarkeit. Im Bereich der Datenschutztechnik gilt der Begriff „linkability“ bzw. „unlinkability“ bereits als länger schon eingeführt (vgl. einführend [Chaum 1985]). Verkettbarkeit soll dabei die Möglichkeit für einen Beobachter bezeichnen, unterschiedliche Ereignisse bezüglich eines Merkmals verbinden zu können (vgl. [Pfitzmann/Hansen 2007]). Verkettung bezeichnet entsprechend ein bereits erfolgtes In-Beziehung-gesetzt-Haben. Konzeptionell besteht der wesentliche Vorzug des Begriffs Verkettbarkeit darin, dass er die wissenschaftstheoretische „Superkategorie“ der Beziehung, im Kontext des Datenschutzes: der Personenbezug, von Symbolen in eine komponentenhaft-operationalisierbare Form überführt. Dadurch wird die Operation des kommunikativ-operativen In-Beziehung-Setzens explizit. Das heißt: Das In-Beziehung-Setzen wird somit beobachtbar, kritisierbar, also immer auch als anders gestaltbar ausgewiesen.

2.3.2.2 Verkettbarkeit von Adressen

Rein logisch kann alles mit allem verkettet bzw. in Beziehung zueinander gesetzt werden, sofern der Verkettungsinstanz (also dem „Verketter“) Bezeichnungen zur Verfügung stehen. Als eine solche Verkettungsinstanz kann man an einen menschlichen oder sozialen Beobachter (Organisation) oder in materialisiert geronnener Form an einen mit vielerlei Sensoren ausgestatteten Computer denken.

Zeichen, die etwas bezeichnen, werden als Symbole (lateinisch für Sinnbild, das Zusammengefügte) bezeichnet. Ein Beobachter bezeichnet mit Hilfe von Symbolen etwas in der Welt. Eine Bezeichnung wird dadurch sozial signifikant, dass sie als Kommunikation aufscheint und durch Kommunikation, mit ihren Formierungsprozessen, sich selbst stabilisiert. Sprache konstruiert die Welt symbolisch und weist mit den (logischen) Mitteln der Sprache über die als solche bezeichnete Faktenwelt hinaus. Bezeichnet werden können neben Artefakten auch andere Symbole sowie Zustände oder Beziehungen, die keinen zeichenhaften oder dinglichen Charakter aufweisen, wie beispielsweise der Zustand des „Verliebt-Seins“, die Beziehung „Vater-sein-von“ oder auch Zeit und Raum. Durch Kontextierungen, die der Beobachter konstruktiv vornimmt, erhält ein Bezeichner eine spezielle Bedeutung.

Aus einer Bezeichnung wird ein Identifikator (engl.: „Identifier“), wenn die Funktion der Bezeichnung, man kann auch sagen: wenn der kommunikative Verwendungszusammenhang des Symbols, für den Beobachter darin besteht, Dieses von Anderem, also den Apfel von der Birne, zu unterscheiden und dadurch Dieses zu identifizieren. Das setzt sowohl auf der bezeichnenden als auch der bezeichneten Seite Eigenschaften voraus: Der Unterschied des Bezeichneten muss im Hinblick auf bestimmte zugesprochene Eigenschaft als stabil erscheinen. Das beobachtende, identifizierende System muss den Identifier zur Unterscheidung im Hinblick auf einen bestimmten Aspekt stabil im (kommunikativen) Gedächtnis und (kommunikativ) zugriffsfähig halten. Ein Identifier setzt somit einen Beobachter, abstrakter formuliert: eine Beobachtung, voraus, der den Akt des Identifizierens im Hinblick auf einen bestimmten Aspekt (lateinisch für Anblick, Ansicht) oder aus einer bestimmten Perspektive operativ stabil vollzieht. Anders formuliert: Es ist immer ein Beobachter, der einen in der Welt seienden Anlass, ein Ereignis mit Hilfe eines Zeichens symbolisiert oder ein bereits daseiendes Symbol (Zeichenvorrat einer Sprache) verwendet und in einen spezifischen Identifier für sich transformiert.

Sobald etwas derart Bezeichnetes oder Identifiziertes in der Lage ist, Einfluss auf die Bezeichnung zu nehmen, man kann auch sagen: sobald die Operation des „Be-Zeichnens“ oder Identifizierens insbesondere auf Seite des Bezeichneten reflexiv wird, lässt sich im Sinne einer weiteren Informationsanreicherung von Adressierung sprechen. Wesentlich dabei ist: Eine Adresse identifiziert (eigensinnige) Operationen und macht diese dadurch zugänglich. Für spezifische Operationen stehen spezifische Adressen zur Verfügung. Adressen fungieren insofern als in Operationen eingepasste Identifier. Die Identifier müssen somit operabel zugänglich (gemacht) sein. Eine Adresse ist ein Bestandteil aus einer „Adressierungsstruktur“, die über ein Regelwerk generiert wird. Man kommt nicht allzu weit, wenn man in das URL-Adressfenster eines Webbrowsers anstelle des Kommunikationsprotokolls und der Serveradresse einen Vornamen, ein Autokennzeichen oder eine geographische Koordinate einträgt. Über jede Regel innerhalb einer Adressierungsstruktur wacht jeweils mindestens eine Organisation. Eine falsche Anwendung der Adressierungsregel führt zum Funktionsverlust, deshalb reichen im Bereich der Kommunikationstechnik Empfehlungen (Requests for Comments (RFC)).

Generalisiert formuliert: Es sind Organisationen, die die Adressen dieser Welt verwalten, also stabil erhalten, zuteilen, und etwaige Kollisionen letztlich auflösen. Noch genereller formuliert: Adressabilität der Welt wird durch Organisationen erzeugt. Eine verbindliche Letzt-Adressabilität der Körper von Personen herzustellen obliegt dabei, im rechtlichen Rahmen des Gewaltmonopols, staatlichen Organisationen. Adressabel sind Personen, Organisationen und Kommunikationstechnik. Dabei wird die Adressabilität sowohl von Personen als auch von Kommunikationstechnik durch die diese umschmiegenden Organisationen gewährleistet. Noch einmal verdichtet formuliert gilt: Keine Adressabilität, keine Beobachtbarkeit, keine Verkettbarkeit ohne Organisation.

Zwischenfazit: Ein Bezeichner bezeichnet. Ein Identifier bezeichnet und unterscheidet und erzeugt durch Unterscheidung „Identität“, wobei bestimmte Eigenschaften sowohl beim Bezeichneten als auch beim Bezeichnenden vorliegen müssen. Eine Adresse identifiziert über Bezeichner bestimmte Operationen im Unterschied zu anderen Operationen. Ein Beobachter beobachtet durch Verkettungen von Bezeichnetem, Identifiziertem und Adressen. Aus spezifischer Datenschutzsicht sind die relevanten Beobachter Organisationen, die neben anderen Entitäten regelhaft adressierbare (also bezeichenbare und identifizierbare) Personen mittels der von Organisationen kontrollierten Operationen verketten.

2.3.2.3 Verkettung durch Kommunikation

Dabei sieht sich der Datenschutz vor das Problem gestellt, über eine Strategie zu verfügen, mit der Verkettungen von Personeneigenschaften durch Organisationen als angemessen oder als nicht angemessen beurteilt werden, und zwar noch vor einer durch Gesetze geregelten rechtlichen Bewertung. Für einen über das Recht als Referenz hinausweisenden Blick lohnt es, die Theorieangebote der Soziologie zu sondieren. Die nachfolgenden soziologischen Überlegungen zur Verkettbarkeit bzw. Verkettung orientieren sich an der aus der soziologische Systemtheorie bekannten Unterscheidung zweier Typen von Sozialsystemen, nämlich dem Systemtyp der Organisation und dem des Sozialsubsystems (vgl. [Luhmann 1997]).

Der Vergleich dieser beiden Sozialsysteme zeigt: Neben der beobachtbaren Tendenz der Durchorganisation moderner Gesellschaften aufgrund eines noch einmal gesteigerten Industrialisierungsschubs durch moderne Kommunikationstechniken, die beispielsweise in Form von Data Warehouses nahezu alles mit allem beliebig und automatisierbar zu verketten gestatten, gibt es eine andere, und zwar gegenläufige und nicht minder wirkungsmächtige gesellschaftliche Tendenz, nämlich die der funktionalen Differenzierung autonom operierender Sozialsysteme. Die funktionale Differenzierung führt zu einer fortgesetzten Entkettung gesellschaftlicher Operationen. Daraus bezieht der Datenschutz seine positiven Leitbilder: den rationalen Kunden, den autonom-eigensinnigen Bürger und ganz allgemein den vernunftbegabten, individuellen Menschen. Es ist diese Differenz der Verkettungsmodi, wie sie Organisationen vornehmen, und sozialen Funktionssystemen, die ihre spezifischen Formen der Verkettung bzw. Entkettung adressierbarer Entitäten ausgebildet haben, die den Datenschutz als institutionalisierten, kritischen Wächter über die latent imperialistischen Organisationen und deren Kommunikationen hat entstehen ließen. Dass dieser zu bearbeitende, strukturelle Konflikt zwischen Verkettungsformen handfest ist, zeigt sich darin, dass sich Datenschutz von einer

„unverbindlichen“ Bürgerbewegung zu einer erwartungsfest sanktionsfähigen Institution entwickelt hat. Der Beobachtungsgegenstand des Datenschutzes besteht aus Kommunikationsbeziehungen, deren Fairness beurteilt wird.

2.3.2.4 Verkettung durch Organisationen

Nach den ersten nunmehr gesetzten Erfahrungen mit dem globalen, die Computer der lokalen Netze vernetzenden Internet zeigt sich, dass ein Transmissionsriemen wie das Internet mit der Möglichkeit nicht des Energietransports, wie die Industrieforschung seit Karl Marx wähnte, sondern des flexiblen Ankoppelns/Abkoppelns von Einzelmaschinen zu einer Gesamtmaschinerie, einen ganz eigenen steuerungsmaschinellen Beitrag zur Industrialisierung leistet. In diesem Sinne fungiert das Internet als global verselbstständigtes großtechnisches System, mit einem World Wide Web und den darauf aufsetzenden Web Services als Maschinen-Verkettungsmaschinerie. Dieses System schickt sich an, durch operativ zugängliche Adressierbarkeit, beispielsweise in Form von RFID-Chips („Radio Frequency Identification“) und ubiquitärer Sensorik, auch außerhalb des Netzmediums und dessen Komponenten zu funktionieren. Diese absehbare Entwicklung erzeugt einen Industrialisierungsschub, der nicht wie bisher primär die Energiemaschinen, sondern vornehmlich die organisiert-industrialisierte Verarbeitung von Kommunikationen betrifft. Spätestens mit dieser Entwicklung breitet sich die an technischer Kausalität orientierte Verkettungen durch Organisationen, die diese Techniken teilweise schon heute nutzen, gesellschaftsweit aus.

Dieser gesellschaftliche Zwang zur Technisierung bzw. regelorientierter automatisierter Beobachtungen der Umwelt von Organisationen durch Organisationen führt dazu, dass Organisationen die eigensinnigen Operationen an den Adressen zu kontrollieren trachten. Das Ziel von Organisationen besteht darin, durch organisierte Aktivitäten kausal kontrollierte Wirkungen bei Personen, in den eigenen Suborganisationseinheiten, anderen externen Organisationen und vor allem der eigenen IT zu erzielen. Und damit wird die operative Autonomie der so Adressierten tendenziell immer unterlaufen. Der Kunde ist in diesem Sinne in der Interaktion mit der Organisation aus Sicht der Organisation genau kein König, sondern Ziel von Werbung und intelligentem Marketing in der Kundenbindung, und der Bürger ist genau so wenig der Souverän, wenn er sich pauschal Verwaltungsentscheidungen zu unterwerfen hat und zum Ziel von Rhetorik und strategischer Kommunikation gemacht wird. Gerade weil sich die Klientel von Organisationen permanent der Kontrolle zu entziehen droht, bemühen sich Organisationen durch Informationstechnik, Identifier für relevante Eigenschaften zu finden, um über zielgenaue Adressierungen Operationen – vornehmlich Zahlungen, politische Entscheidungen und Weltsichten – automatisiert zu erfassen, zu speichern, zu analysieren und entsprechend zielgenau zu bearbeiten.

Durch den Ausbau universalisierter Vernetzungstechniken (in konkreter Form etwa als Internet, Bluetooth, WLAN), universalisierter Adressierbarkeiten (in konkreter Form etwa als URI („Universal Resource Identifier“), Internet Protocol Version 6, RFIDs) sowie standardisierter Operationen und Datentransfers (XML, Web Services, Java Beans oder .net) so entsteht vielfach die Vorstellung, dass die Bürger und Kunden mit Hilfe dieser neuen Techniken unter ein durchindustrialisiertes, einseitiges Organisationsregime gezwungen würden, das deren ohnehin fragile Souveränität als Staats- und Marktmacht untergrübe. Die damit einhergehenden gesellschaftlichen Risiken bzw. individuellen Gefahren bestehen auch tatsächlich und zweifelsfrei. Denn an der Verbreitung dieser Adressierungs- bzw. Verkettungstechniken zweifelt allein aufgrund der einleuchtenden immensen ökonomischen Vorteile niemand ernsthaft. Der etablierte Begriff von der „Industriegesellschaft“ bestärkt dabei die Vorstellung, dass die für Organisationen typischen Verkettungsformen von Techniken und Menschen mit den Operationen von Organisationen umstandslos auch auf Gesellschaft als Ganze hochrechenbar seien. Allerdings greift diese Vorstellung zu kurz, in diesem Sinne von der Industriegesellschaft – oder natürlich ebenso von einer postindustriellen Gesellschaft, was in mehrfacher Hinsicht fragwürdig ist – zu sprechen. Denn dies hieße, Gesellschaft im Sinne einer (Super-) Organisation aufzufassen, die als von einem Punkt aus kontrollierbar erschiene, etwa im Sinne einer „Nationalgesellschaft“, in der die Regierung festlegt und vor allem kontrollieren kann, was zu geschehen hat. Die moderne soziologische Systemtheorie teilt eine solche Vorstellung einer derart durchorganisierten Gesellschaft nicht. Vielmehr spricht sie von einer Evolution sozialer Subsysteme, deren Systeme zueinander in keinem Über- oder Unterordnungsverhältnis stehen (vgl. [Luhmann 1997]). Die Evolution dieser Subsysteme erfolgt dabei auf einer anderen Ebene als die Evolution der

Organisationen der Gesellschaft und läuft der Industrialisierungstendenz insofern entgegen, als dass sich diese sozialen Systeme durch funktionale Konzentrationen auf spezifische Binärcodes voneinander entkoppeln.

Zwischenfazit: Während Organisationen ihre Umwelt latent unter ihre Kontrolle zu bringen versuchen, indem sie transaktionskostensenkend auch ihre externe Klientel im Modus von Quasimitgliedern den organisationsinternen Entscheidungsverfahren und autonomieeinschränkenden Personenbezügen zu unterwerfen trachten, müssen die Sozialsubsysteme an ihren zentralen Konfliktstellen etwaige Personenbezüge kappen.

Was es mit dem Kappen als „Entkettung gesellschaftlicher Operationen und Personenbezüge“ auf sich hat, ist Thema des folgenden Abschnitts.

2.3.2.5 Entkettungs-Verkettungen durch funktional differenzierte Sozialsysteme

Die moderne soziologische Systemtheorie unterscheidet drei Typen an Sozialsystemen, die sich durch eigensinnige Entwicklungsdynamiken auszeichnen: Interaktionssysteme, Organisationssysteme und Gesellschaftssysteme (vgl. [Luhmann 1997]). Während Organisationen ihre Systemgrenzen erzeugen durch die Unterscheidung von Mitgliedern und Nichtmitgliedern in Bezug auf die Beteiligung an Entscheidungskommunikation, beschreiben die Termini der funktionalen Differenzierung und der autopoietischen Reproduktion die spezielle Grenzziehung der gesellschaftlichen Subsysteme Ökonomie, Recht, Politik und Wissenschaft: Diese werden aufgefasst als funktional zugespitzte Kommunikationssysteme, die außer durch sich selbst von keiner anderen Instanz aus steuerbar sind.[34]

In der Moderne brechen gemäß der Theorie funktionaler Differenzierung die traditionell hierarchischen Beziehungen zwischen der Politik und Religion und dem Rest der Welt, also insbesondere dem Recht, der Wissenschaft und der Wirtschaft auf. Als Beispiele seien nur die allseits bekannte Emanzipation eines primär ökonomisch orientierten Bürgertums vom politisch verankerten Adel, für das insbesondere die französische Revolution steht, oder die mit dem Namen Atatürk verbundene Trennung von Religion und Politik in der Türkei genannt. Jedes der sozialen Subsysteme, die man sich als reine Kommunikationssysteme vorstellen muss, schließt sich kognitiv selbstbezüglich ab und konzentriert sich funktional auf sich selbst. Der Erfolg wirtschaftlichen Handelns wird ökonomisch allein an der Verzinsung des Kapitals beobachtet, nicht etwa länger an der Gottgefälligkeit oder der patriotischen Gesinnung oder der wissenschaftlichen Fruchtbarkeit von Zahlungen. Das Rechtssystem beobachtet die gesamte Welt allein unter der Differenz von Recht und Unrecht. Nicht Moral und Ethik, sondern positiv formuliertes Recht steuert die Entwicklung weiterer Rechtssätze. Politik wird entlang der Differenz von Macht und Nichtmacht kommuniziert, mit Positionskämpfen als für Menschen beobachtbaren Handlungsformen. Die ökonomische, rechtliche oder wissenschaftliche Umwelt wird als Störung vom politischen System wahrgenommen und kann politisch nur bearbeitet werden, wenn sich diese bei Nachhaltigkeit in Machtfragen übersetzen lassen. Und Wissenschaft interessiert sich allein für die methodische Entscheidbarkeit von Aussagen bezüglich der Behauptbarkeit von Wahrheit, alles andere, insbesondere (externe) Verpflichtungsversuche auf gute Moral, auf religiöse Absicherung, auf politische Passgenauigkeit oder ökonomische Verwertbarkeit, werden als Perturbationen aus der Umwelt und damit als Pathologien des wissenschaftlichen Diskurses thematisierbar.

Um die Verkettungsmodi der sozialen Funktionssysteme genauer zu verstehen, gilt es, die Verkettbarkeit bzw. Verkettung von Ereignissen im Hinblick auf interne oder externe Verkettungen zu unterscheiden. Zunächst zu den systeminternen Verkettungen, die man sich wie folgt vorstellt: Die Systeme reproduzieren sich anhand binärer Codes, die als symbolisch generalisierte Kommunikationsmedien fungieren und als solche im Vollzug der Verkettung die gesellschaftliche Form von

[34] Soziales gilt modernen Soziologen als eine „Realität sui generis“ (vgl. [Durkheim 1984[). Das heißt, dass die eigensinnige Dynamik der sozialen Welt soziologisch nicht aus dem Denken, Handeln und Sprechen oder gar aus einem Wesen des Menschen heraus zu beschreiben und erklären ist. Vielmehr sehen sich Soziologen aufgefordert, Soziales nur aus Sozialem zu verstehen und zu erklären. Auf die Diskussion der hochinteressanten Eigenschaften von Interaktionssystemen im Hinblick auf Verkettbarkeit kann mangels Platzes hier nicht eingegangen werden.

Beobachtung sind: Zahlungen/Nichtzahlungen mit Preisen als ökonomisches Programm; Recht/Unrecht mit Gesetzen als rechtliches Programm; Macht/Nichtmacht mit Programmatiken als politisches Programm; Wahr/Falsch mit Theorien und Methoden als wissenschaftliches Programm. Ereignisse als verkettbare Komponenten werden in diesen sozialen Codes bezeichnet und auf diese Art und Weise sozial beobachtbar. Diese binären Schematismen strukturieren mögliche kommunikative Anschlüsse universell und dadurch formal perfekt, ohne sie deshalb schon inhaltlich festzulegen. Es kann praktisch alles auf der Welt spezifisch ökonomisch, rechtlich, politisch oder wissenschaftlich thematisiert werden. Offen ist aber, in welcher Höhe ein Preis gezahlt/nicht-gezahlt wird, welches der Gesetze letztlich den Ausschlag für die Entscheidung über Recht oder Nichtrecht gibt, welche der verschiedenen politischen Programmatiken durchgesetzt wird oder welche der vielen Theorien oder Methoden für die Wahrheitsfindung die richtige ist. Entscheidend ist: Jeder Vollzug einer (Nicht-)Zahlung reproduziert Nachfolgezahlungen, an jede gesetzliche oder politische Entscheidung knüpfen weitere gesetzliche oder politische Entscheidungen an, jede wissenschaftlich behauptete Wahrheit unterliegt weiterhin einem latenten Zweifel.[35] Und sehr wesentlich für unseren Zusammenhang: Entscheidungen in einem System schlagen nicht zwangsläufig auf Entscheidungen im anderen System durch.

Deshalb nun zu den systemexternen Verkettungen. Systemexterne Verkettungen, die man traditionell als „Beziehungen“ zwischen den Systemen bezeichnen würde, bilden keine festen Verkettungen untereinander. Sie bilden auch Schnittmengen aus oder importieren oder exportieren auch keine verkettbaren Komponenten zwischen den Systemen. Zwischen den Systemen gibt es ferner keine Form einer konflikthaften-widersprüchlichen Vermittlung, wie man sie sich im traditionell dialektischen Sinne vorstellen könnte. Jede Umweltbeobachtung durch ein System kann immer nur anhand des geschlossenen, systemeigenen Codes erfolgen. Man kann auch sagen: Die gesellschaftlichen Funktionssysteme verstehen nur sich selbst. Kontakte zwischen Systemen geschehen stattdessen nur ereignishaft punktuell, als „zeitpunktbezogene Einheit“. Für einen Moment beobachten die Systeme ein solches punktuelles Ereignis synchron.[36]

Als Beispiele für diese nicht leicht verständlichen Verkettungsmodi der Sozialsubsysteme untereinander seien Steuerzahlung und Gutachten angeführt, die sowohl im politischen wie im ökonomischen System anschlussfähig sind, allerdings ganz unterschiedlich: Im Moment der Zahlung von Steuern als Ereignis berühren sich das ökonomische und das politische Kommunikationssystem. Gezahlte Steuern thematisiert das politische System dann politisch allein unter dem Aspekt des Erhalts der Fortsetzbarkeit politischer Gestaltungsmöglichkeiten – und sei dies in Bezug auf die eingeschlagene Wirtschaftspolitik. Das ökonomische System thematisiert Steuern allein unter dem Aspekt der Kosten, dass Nichtsteuernzahlen kapitalzinslich beurteilt teurer würde als Steuern zu zahlen. Man kann sich das als ein Schema der Kommunikation vorstellen, das Ökonomen, die in Marktunternehmen arbeiten, zwangsläufig zu nutzen haben. Das ist keine Frage ihres persönlichen kognitiven Talents, sondern eine sozialstrukturell massenhaft induzierte Kalkulationsform.

Bei wissenschaftlichen Gutachten für politische Organisation verliert der Gutachter seine Reputation schlagartig, wenn er das Gutachten nicht nach ausschließlich wissenschaftlichen Standards für Wahr-

[35] Die Verfasser möchten hier an die seit Mitte der 90er Jahre geführte Diskussion über Experimente erinnern, wonach die Ausbreitung von „Information“ mit Lichtgeschwindigkeit offenbar doch nicht die schnellstmögliche ist.

[36] Diese Theorie der kognitiven Geschlossenheit autopoietisch operierender Systeme, wonach nur durch Geschlossenheit konstruktive Offenheit erzeugt werden kann, wurde erfolgreich zum ersten Mal von Biologen angewendet, die das kognitive System von Fröschen untersuchten (vgl. [Manturana 1982]). Diese Theorie, die eine ganz neue Form von Verkettbarkeit mit empirischen Belegen vorstellbar machte, traf sowohl auf erste mathematische Formalisierungen „chaotischer“ Systeme („Mandelbrot- und Juliamenge“) als auch auf naturwissenschaftlich orientierte Selbstbezugstheorien à la „seltsame Schleifen“ [Hofstadter 1985]. Die komplexe Figur des Selbstbezugs war durch die Aufklärung der Deutschen Hochphilosophie, namentlich durch Fichte, Kant, Schelling, Hegel und Marx, bereits sehr differenziert vorbereitet und von Logikern und Sprachtheoretikern wie Whitehead, Russel, Tarski und Wittgenstein zugespitzt worden. Neu ist an der modernen Diskussion zur Selbstreproduktion von Systemen die Orientierung an Elementarereignissen als, wie wir nun sagen können: verkettbare Systemkomponenten. Nicht der logisch latent beunruhigende Selbstbezug an sich, sondern der Komponentencharakter von Kommunikationen als Elementarereignissen ist dasjenige, was an dieser Theorie das Bemerkenswerte ist und die Vorstellung von „Beziehungen“ respektive „Personenbezug“ operativ zugänglich macht.

heitskonstruktion anfertigt. Damit er auch weiterhin als Wissenschaftler arbeiten kann, muss er auf das Festigen seiner wissenschaftlichen Reputation durch Ausweis seiner an Wahrheit orientierten Wissenschaftlichkeit gerade auch in Gutachten achten. Rhetorik, die die Differenz von Wahr und Falsch politisch zudeckte, ist nicht zugelassen. Politisch wird ein wissenschaftliches Gutachten dagegen nur dann publiziert und in die an Macht orientierte Auseinandersetzung geworfen, wenn sich ein Politiker davon versprechen kann, dass es in die politische Programmatik passt, vollkommen ohne Berücksichtigung des wissenschaftlichen Gehalts.[37] Auch das ist keine Frage eines besonderen mentalen Talents oder einer Moral aller Beteiligten, sondern sozial induziert, allseits akzeptiert und allgemein erwartbar.

Die Systeme sind aufgrund ihrer kognitiven Geschlossenheit auf ihre internen Quellen der Informationsbeschaffung angewiesen. Neben den Störungen aus ihren Umwelten, die die Systeme für sich in systemeigen-konstituierte Informationen umsetzen müssen, reagieren die Systeme deshalb vor allem auf ihre systeminternen Quellen der Verunsicherung: Die Ökonomie kennt den unberechenbaren Markt mit dem Kunden als König; das Recht kennt die Legislative, den moralisierenden Richter und den präsidialen Gnadenakt; die Politik kennt die Wahl, den Willen des als souverän begriffenen Staatsbürgers, die politische Rhetorik und die opportunistische öffentliche Meinung; die Wissenschaft kennt den herrschaftsfreien Diskurs und den eigensinnig-vernunftbegabten aber triebgeleiteten Menschen, bei dem sich fortgesetzt zeigt, das Wissen und Gewissheit nicht in eins zusammenfallen. Und die Systeme kennen keine Adressen und sind ihrerseits nicht adressierbar. Sie bieten die Leitdifferenzen für die Entscheidungen adressabler Organisationen und Personen.

Zwischenfazit: Die sozialen Funktionssysteme verstehen einander nicht, sind zueinander nicht hierarchisch anordenbar und können einander deshalb auch nicht im Sinne kausaler Steuerungen kontrollieren. Es verbleibt nur, dass sie sich gegenseitig spezialisierte und zugriffsfeste Komplexität bieten. Ihre Sensorik für Umwelt besteht darin, dass sie systeminterne Mechanismen kausaler Selbstverunsicherung ausgebildet haben. Sie versorgen adressable Organisationen und Personen mit Entscheidungsmaterial.

Im Vergleich zu Organisationen zeigt sich aus einer steuerungs- bzw. kontrollorientierten Perspektive heraus, dass diese Sozialsysteme ihre eigenen Quellen der Unsicherheiten nicht bekämpfen, sondern aufwändigst zu pflegen haben. Denn diese Quellen stellen die verlässlichsten systemeigenen Sensoren für sich und die Umwelt dar. Sie bieten keine Adressabilität, sie müssen schon deshalb allesamt auf Personenbezüge verzichten bzw. aktiv Vorkehrungen treffen, um Verkettungen zu unterlassen, indem sie Personenbezüge kappen: Man denke an die programmatische Weisung durch Justitia, ohne Ansehen der Person Recht zu sprechen; man denke an das aufwändige Herausrechnen des Wissenschaftlers aus dem Erkenntnisprozess, um Allgemeingültigkeit der Erkenntnisse beanspruchen zu können; man denke an das allgemeine und geheime Wahlrecht, das sozial den Austausch politischer Programme und psychisch das „Nein, so nicht weiter!“-Sagen ermöglicht; man denke an die Schlichtheit von Zahlungen mit Bargeld ohne Geschichte und unbekannter Herkunft, Markt pur.

Die Funktionssysteme der Moderne sind somit an ihren ganz zentralen Konfliktstellen auf Pseudonymität (im Sinne des „ohne Ansehen der Person“) oder Anonymität (des Wissenschaftlers, des Wählers, des Kunden) – also das Unter-Bedingungen-Stellen oder sogar gedächtnislose Kappen von Verkettbarkeiten – angewiesen, gestört aber auch realisiert durch Organisationen, die genau diese aus ihrer Sicht riskanten Verkettungsmodi der Pseudonymisierung und Anonymisierung permanent zu unterlaufen versuchen (vgl. [Rost 2003]).

Wie bereits dargestellt unterlaufen Organisationen dieses für die moderne Gesellschaft charakteristische Kappen von Bezügen auf konkrete Personen permanent. Organisationen verfolgen ihre gegenläufigen Funktionsprimate: Ihre Ordnungsstrategien richten sich auf die Herstellung von Entscheidungen aus, wofür Hierarchisierungen mit kontrollierten Steuerungsmöglichkeiten funktional sind. Sie

[37] Natürlich gibt es Gefälligkeitsgutachten – aber diese haben ihre Grenzen. Das hat man eindrucksvoll in Bezug auf die Salzstöcke in Gorleben gemerkt, als nach einer Gutachterschlacht am Ende ein wirklich wissenschaftliches Gutachten hermusste, um die Risiken der Atommülleinbringung tatsächlich juristisch, politisch und ökonomisch kalkulieren zu können. Und auch in Russland mochte man die dialektisch offenbar nicht in den Griff zu bekommende Quantenphysik ab 1956, also mit der Chrustschowschen Entstalinisierungswende, nicht mehr ignorieren; schließlich konnte man nicht Gefahr laufen, über keinen Atomphysikernachwuchs mehr zu verfügen.

beobachten die Aktivitäten anderer Organisationen sowie die geschiedenen Funktionalitäten der sozialen Subsysteme, die internen und externen Interaktionssysteme sowie nicht zuletzt ihr personales Inventar und ihre externe Klientel. All dies müssen sie miteinander synthetisieren. Das bedeutet: Organisationen sind die Verkettungsmaschinen schlechthin.

Diese zugleich ebenso riskante wie großartige Syntheseleistung gelingt Organisationen, indem sie die Welt der Dinge, des Sozialen und des Menschen füreinander adressierbar und dadurch in Verfahren kausal einbindbar machen. Jedes Ding dieser Welt, jede soziale Einheit und jeder einzelne Mensch erhält erst durch Organisationen einen gesellschaftlich relevanten Bezeichner bzw. Namen und wird dadurch als Adresse identifizierbar. Bei organisationsinternen Adressen ist in der Regel eine organisiert-kontrollierbare Intelligenz gefragt, die der Organisation Beobachtungsvorteile gegenüber ihrer Umwelt verschafft. Bei organisationsexternen Adressen schätzen Organisationen dagegen primär Erwartungssicherheit durch kausale Zugänglichkeit: Organisationen können es sich nicht aussuchen, ihre Umgebung kontrollieren zu „wollen".

Doch zugleich operieren Organisationen in einer Umwelt, in der die Schemata der Funktionsprimate für Organisationen – also der primären Orientierung an der Kapitalverzinsung durch Firmen, der Machtdurchsetzung durch an Recht orientierte Verwaltungen, des Machtausbaus durch politische Organisationen und der diskursiven Unabgeschlossenheit durch Wissenschaftsinstitutionen – durch sehr stabile, verselbstständigte Sozialsysteme ebenso als Kontext vorgegeben ist wie individualisierte Menschen, die zunehmend selektiver ihre Aufmerksamkeit an Organisationen binden. Obwohl Organisationen aus Sicht der Einzelpersonen die Strukturen der Sozialsubsysteme durch Allverkettungen latent unterlaufen, reproduzieren gerade sie im Ergebnis marktorientierte Zahlungen, legitime Machtkonstellationen, legale Rechtsregimes und ergebnisoffene Diskurse. Aber nur, wenn zugleich die kausale Ungewissheiten erzeugenden Entkettungsmechanismen des Marktes, des sich selbst gegenüber skeptisch seienden Rechtsstaates (der deshalb nebenbei bemerkt Datenschutz-Institutionen ausgebildet hat), der opportunistischen öffentlichen Meinung und der Demokratie sowie des latent ergebnisoffenen wissenschaftlichen Diskurses der sozialen Funktionssysteme bestehen bleiben.

2.3.2.6 Adress-Provider, Datensammler und Verketter

Eine weitere Differenzierung soll angeschlossen werden, um den Umgang mit adressablen Entitäten, also deren Generierung und Verwendung, unter dem Aspekt der Verkettbarkeit thematisieren zu können:

Adressierbarkeit stellen Organisationen dadurch her, indem sie Zeichen im Sinne von Identifikatoren zuordnen. Von Adressen soll, wie oben dargelegt nur dann gesprochen werden, wenn Operationen identifiziert werden. So stellen Eltern Adressierbarkeit durch die Namensgebung ihres Kindes her, die allerdings vom Meldeamt sanktioniert werden muss, um gesellschaftlich relevante Gültigkeit zu erlangen. So ist es nicht zugelassen, als Vornamen eines Kindes etwa „Firlefanz" oder vielleicht sinnigerweise „Doktor" zu nennen. Organisation weisen beispielsweise Laufzeichen, Steuerkennzeichen, E-Mail-Adressen, IP-Adressen oder Kunden- und Patientennummern zu. Dies machen sie anhand sozial bereits etablierter Adressierungsstrukturen oder Adressschemata. Organisationen stellen somit nicht nur Adressen, sondern Adressierungsräume her bzw. bauen vorhandene aus. Wobei es aus theoretisch geleiteter Sicht angemessener wäre, anstatt von einem Adressierungsraum von einer Adressierungsdomain zu sprechen, weil eine Domain mehrdimensional sein kann und nicht einer am Raum orientierten Logik unterliegen muss. Organisationen agieren, vermittelt durch die Sensorik von Personen, Maschinen und nicht zuletzt anderen Organisationen, in diesem Sinne als „Adress-Enabler" (d.h. Adress-Provider basierend auf einem Adressschema von einem Adressschema-Provider). Organisationen sind dafür angewiesen auf Beobachtungen.

Beobachtung bezeichnet ein Registrieren von Unterschieden, das durch Bezeichnung in eine gesellschaftliche Form gebracht wird. Es sind Personen oder Maschinen oder (Sub-)Organisationen, die ihre Beobachtungen in den Workflow von Organisationen einspeisen. Sowohl die Beobachtungen, wie sie der kognitive Apparat von Personen, oder die Beobachtungen, wie sie die Sensorik von Maschinen erzeugen, transformiert eine Organisation in sozial relevante und signifikante Kommunikation. In vielen Fällen wird diese Transformation den Organisationen dadurch leicht gemacht, indem ihnen Mitteilungen von Personen oder anderen Organisationen angeliefert werden. Organisationen

übernehmen zu einem ganz überwiegenden Anteil das Adressierungsmaterial, das andere Organisationen, die als Adress-Enabler agieren, anliefern. Indem Organisationen an Adressen bestimmte Eigenschaften erheben und speichern und diese auf Operationen rückschließen, agieren sie als Beobachter und Datensammler (engl.: „Observer“ und „Data collector“).

Als Verkettung lässt sich, nunmehr höherauflösend als noch zu Beginn, die Synthetisierung von Beobachtungen an einer bestimmten Adresse unter einem bestimmten Zweck bezeichnen. Verkettung sorgt in diesem Sinne für eine Ausrichtung von kommunikativ (und mental) zugänglichen Beobachtungen. Oder anders formuliert: Verkettungsinstanzen (engl.: „Linker“ oder „Concatenator“) beobachten im Hinblick auf einen bestimmten Zweck. Verwaltungen verketten im Hinblick auf die Rechtmäßigkeit von Kommunikationen und Handlungen, Unternehmen im Hinblick auf eine optimale Kapitalverzinsung, wissenschaftlich orientierte Institute im Hinblick auf Wahrheitsfähigkeit, politisch agierende Organisationen im Hinblick auf Machterhalt oder Machtausbau.

Die dafür brauchbaren Verkettungsmodelle liefern wiederum Organisationen an, die diese Modelle ausrichten an dem Primat, unter dem sie die Konflikte typischerweise eben auflösen, um als Organisationen fortzubestehen: also ihre Verkettungen entweder primär referenzierend in Bezug auf Rechtmäßigkeit, Kapitalverzinsung, Wahrheit oder Macht. Organisationen müssen all diesen vier Funktionsansprüchen genügen, doch werden diese unter jeweils einem Primat aufeinander bezogen. Ein Unternehmen wird dadurch zum Organisationstypus „Unternehmen“, nur deshalb, weil es sich an der Kapitalverzinsung des eigenen Tuns ausrichtet, und die anderen Funktionsansprüche dafür in den Dienst nimmt.

2.3.2.7 Informationelle Selbstbestimmung in Bezug auf Verkettbarkeit

Es wurden zwei gesellschaftliche Verkettungsmechanismen aufgezeigt, deren Auswirkungen auf Personenbezüge gegenläufig sind und die dadurch das Spannungsfeld aufbauen, in dem sich die Arbeit der Datenschutz-Institutionen bewegt: Organisationen verketten kausal mit der latenten Tendenz, auf der Basis einer noch einmal drastisch effektivierten Industrialisierung diesen Verkettungsmodus auch mit Komponenten aus der Umwelt, gegenüber allem und jedem, durchzuhalten. Dagegen verketten die Sozialsubsysteme systemintern über primitive binäre Schematismen (erwartungs-)fest, aber ergebnisoffen,[38] und systemextern punktuell, ohne die Möglichkeit, systemeigene Direktiven in die Präferenzschemata der anderen Subsysteme zu exportieren. Aus Sicht von Organisationen entketten die Funktionssysteme der modernen Gesellschaft.

Es sind die Programmatiken der Subsysteme, die die Figuren des souveränen Bürgers und Kunden gesellschaftlich unwiderstehlich implementieren – und das ohne die funktionale Notwendigkeit eines bestimmten Personenbezugs! Zugleich sind es gerade die Organisationen, die unverzichtbar die Synthese von Personen und funktional differenzierten Sozialsubsystemen herstellen, bei der Personenbezüge unabwendbar anfallen. Der Datenschutz sieht sich aufgerufen, in jedem Einzelfall die Risiken und die Chancen, die in den organisierten Verkettungen für Personen liegen, zu beurteilen bzw. formend auf diese Einfluss zu nehmen.

Zuletzt: In dieser Situation ist Identitätsmanagement, als Umsetzung des Konzeptes der nutzerkontrollierten Verkettbarkeit, möglicherweise ein aussichtsreicher Kandidat, um diese latent konfliktbehaftete Gemengelage handhabbar zu machen (vgl. [Hansen/Rost 2003]). Stünde Bürgern[39], Kunden und Organisationsmitgliedern ein nutzergesteuertes Identitätsmanagementsystem zur Verfügung, so fungierte dieses auch als eine Art persönliches Gegenfeuer zur Bekämpfung des Flächenbrands voll-

[38] Solche logisch undurchsichtigen, ja beunruhigenden und öffentlich-diskursiv kaum zugelassenen Aussagen lassen sich nicht vermeiden. Sie zeigen an, dass wir wissenschaftstheoretisch neuer Logiken bedürfen, zumal das Versprechen einer „operationalisierungsfähigen Dialektik“ (vgl. [Günther 1978]) bis heute trotz aufwändiger Versuche nicht eingelöst wurde. Soziologisch ist es nicht allzu überraschend, wenn mit großen gesellschaftlichen Veränderungen auch neue Logiken, deren diskursive Zwangsläufigkeiten als unbestreitbar akzeptierbar gelten, entstehen.

[39] Auf die Grenzen der Pseudonymisier- und Anonymisierbarkeit in Bezug speziell auf E-Government verweist Gundermann (vgl. [Gundermann 2003]). Das hier die Grenzen für die Verwendung von Pseudonymen tatsächlich besonders eng gezogen sind mag u.a. auch daran liegen, dass sich die Besonderheit staatlicher Souveränität darin auszeichnet, bis auf die Körper der Bürger durchgreifen zu können.

ständig durchindustrialisierter Organisationen der Gesellschaft. Man müsste sich als Bürger und Kunde nicht nur auf die positiven Effekte des Marktes, der Rechtsprechung, der öffentlichen Meinung und des wissenschaftlichen Diskurses verlassen.

Eine weitere und vielleicht überraschende Folge des technischen Starkmachens des Nutzers im Hinblick auf Kontrolle von Verkettbarkeiten könnte darin bestehen, dass es guten Sinn macht, Einzelpersonen als Daten verarbeitende Stellen aufzufassen. Wie Organisationen wären Einzelpersonen professionell mit ökonomischen Risiken, Compliance-Anforderungen und permanenter technischer Aufrüstung der Organisation ihrer gesellschaftlich relevanten Kommunikationen befasst. Das sucht sich natürlich so niemand aus, es ist eine alles andere als „gemütliche Vorstellung“, sie wird den Bürgern und Kunden, den Menschen gesellschaftlich schlicht aufgezwungen. Im Ergebnis bestünde für Personen dann die Chance, auf Augenhöhe mit Organisationen datensparsam und zweckgerichtet nur dasjenige verkettbar zu kommunizieren, was funktional zugespitzt unabdingbar ist. Das Recht auf Datenschutz wäre dann als ein „Recht auf informationelle Selbstbestimmung in Bezug auf Verkettbarkeit“[40] für alle Beteiligten gleichermaßen gestaltbar umgesetzt.

2.3.3 Juristische Grundlagen

2.3.3.1 Rechtliche Einordnung von Verkettung/Verkettbarkeit

2.3.3.1.1 Einführung

Wenn man die Begriffe Verkettung („linkage“) bzw. Verkettbarkeit („linkability“) aus juristischer Sicht betrachten möchte, fällt zunächst einmal auf, dass diese Termini weder vom Gesetz definiert oder auch nur verwendet werden noch bislang breiteren Eingang in die juristische Fachliteratur gefunden haben[41]. Vielmehr handelt es sich bei diesen beiden Begriffen um solche, die sich im Rahmen des technischen Diskurses zu Datenschutz und Datensicherheit herauskristallisiert haben[42].

Nachfolgend wird der Versuch unternommen, sich dem Phänomen der Verkettung aus juristischer Sicht zu nähern. Hierfür werden die folgenden Definitionen von Verkettung und Verkettbarkeit zugrunde gelegt:

- Verkettung ist eine Zusammenführung von Daten mittels identifizierender Merkmale oder Pseudonyme.
- Verkettbarkeit bezeichnet hingegen schon die bloße – theoretische – Möglichkeit, unterschiedliche Daten mittels identifizierender Merkmale oder Pseudonyme zusammenzuführen.

2.3.3.1.2 Volkszählungsurteil

Als Ausgangspunkt für die Überlegungen zur rechtlichen Einordnung des Begriffs der Verkettung soll das Volkszählungsurteil[43] des Bundesverfassungsgerichts dienen, welches das deutsche Datenschutzrecht entscheidend geprägt hat. In diesem Urteil hat das Gericht erstmals die Existenz eines Grundrechts auf informationelle Selbstbestimmung anerkannt. Dieses Grundrecht stellt eine spezielle Ausprägung des Allgemeinen Persönlichkeitsrechts des Art. 2 I i.V.m. 1 I Grundgesetz (GG) dar und gibt dem jeweiligen Grundrechtsträger die Befugnis, grundsätzlich selbst über die Preisgabe und

[40] Es ist diese Erweiterung „in Bezug auf Verkettbarkeit“, die die datenschutzrechtlich wohlfeile Formulierung „informationelle Selbstbestimmung“ soziologisch überhaupt erst verdaubar macht.

[41] An diesem Befund von [Rost 2004] hat sich zwischenzeitlich nichts Entscheidendes geändert. Ein Gegenbeispiel aus der juristischen Literatur stellen etwa [Roßnagel/Scholz 2000] dar, wo ausführlich auf Verkettung/Verkettbarkeit eingegangen wird.

[42] Eine Definition des Begriffs „unlinkability“ findet sich etwa in den Common Criteria (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik), die unter http://www.bsi.de/cc/ abgerufen werden können (letzter Zugriff im Oktober 2007). Hinsichtlich der im Verkettungsumfeld relevanten Terminologie wird auf [Pfitzmann/Hansen 2007] verwiesen.

[43] Urteil vom 15.12.1983: BVerfGE 65, 1 = NJW 1984, 419.

Verwendung seiner persönlichen Daten zu entscheiden. Mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar wäre dem Gericht zufolge eine Rechts- und Gesellschaftsordnung, in der die Bürger nicht mehr erkennen können, wer was wann und bei welcher Gelegenheit über sie weiß.

Untersucht man nun die Gründe des Volkszählungsurteils im Hinblick auf die Begriffe Verkettung und Verkettbarkeit, so muss man feststellen, dass diese Termini von dem Gericht nicht verwendet worden sind. Interessant erscheint aber eine Passage des Urteils, in der das Bundesverfassungsgericht zu dem Schluss kommt, dass es unter den Bedingungen der modernen Datenverarbeitung kein belangloses Datum mehr gebe[44]. Entscheidend sei nicht die Art der jeweils in Rede stehenden Angaben, sondern die Nutzbarkeit und die Verwendungsmöglichkeiten dieser Daten:

„Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein 'belangloses' Datum mehr.“[45]

Das Gericht verwendet hier den Begriff der Verknüpfungsmöglichkeit(en), der zumindest eng mit dem Terminus der Verkettbarkeit verwandt ist. Darüber hinaus kann man wohl sogar davon ausgehen, dass das Bundesverfassungsgericht mit dem Begriff der Verknüpfungsmöglichkeit das Gleiche bezeichnen wollte wie das, was Techniker unter Verkettbarkeit verstehen. Damit wären auch die Begriffe Verknüpfung und Verkettung inhaltlich deckungsgleich.

Auch der Begriff Verknüpfung resp. Verknüpfungsmöglichkeit hat als solcher keinen Eingang in die geltenden Datenschutzgesetze gefunden. Allerdings enthält die einschlägige juristische Kommentarliteratur (kurze) Passagen, die Ausführungen zu dem Terminus Verknüpfung beinhalten[46]. Danach stellt das Verknüpfen personenbezogener Daten dann ein Verändern dieser Daten im Rechtssinne[47] dar, wenn diese durch ihre Zusammenführung einen neuen, veränderten Informationsgehalt bekommen. Sofern dies nicht der Fall ist, handelt es sich bei der Verknüpfung um ein Nutzen[48] der in Rede stehenden Daten.

Wegen der soeben konstatierten inhaltlichen Deckungsgleichheit von Verknüpfung und Verkettung können diese Aussagen zur Verknüpfung von Daten auch für die rechtliche Einordnung des Begriffs Verkettung fruchtbar gemacht werden. Aus datenschutzrechtlicher Sicht gelten damit für eine Verkettung von Daten die folgenden Grundsätze:

2.3.3.1.3 Anwendbarkeit der Datenschutzgesetze: Personenbezug

Zunächst einmal ist festzustellen, dass der Anwendungsbereich der Datenschutzgesetze nur dann eröffnet ist, wenn personenbezogene Daten verkettet werden[49]. Bei solchen handelt es sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person[50]. Dabei macht der Begriff „bestimmbar“ deutlich, dass der Personenbezug von Daten relativ ist, das heißt, dass in jedem Einzelfall anhand der Kenntnisse, Mittel und Möglichkeiten der Daten verarbeitenden Stelle beurteilt werden muss, ob diese die Daten einer natürlichen Person zuordnen kann (Relativität des Personenbezugs). Ein Personenbezug ist dementsprechend dann zu

[44] Das Bundesverfassungsgericht unterscheidet insofern auch nicht zwischen sensiblen und weniger sensiblen Daten – im Rahmen der Umsetzung der EU-Datenschutzrichtlinie 1995/46/EG ist allerdings der Begriff der besonderen Arten personenbezogener Daten in das Bundesdatenschutzgesetz eingeführt worden (vgl. § 3 Abs. 9 BDSG). Insofern ist nunmehr zwischen „normalen“ personenbezogenen Daten und „besonders schutzwürdigen“ personenbezogenen Daten zu differenzieren.

[45] BVerfGE 65, 1 (45).

[46] Vgl. etwa [Gola/Schomerus 2005, § 3 Rn. 30]; Ehmann in [Simitis 2006, § 29 Rn. 210 ff.].

[47] Siehe die entsprechende Legaldefinition in § 3 Abs. 4 Nr. 2 BDSG.

[48] Siehe die Legaldefinition in § 3 Abs. 5 BDSG.

[49] Vgl. nur § 1 Abs. 2 BDSG. Auch alle anderen Datenschutzgesetze setzen einen Personenbezug der verarbeiteten Daten voraus.

[50] So die Legaldefinition in § 3 Abs. 1 BDSG. Die LDSGe enthalten jeweils deckungsgleiche Definitionen (vgl. z.B. § 2 Abs. 1 LDSG SH).

bejahen, wenn die verantwortliche Stelle den Bezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand herstellen kann[51].

Im Übrigen besteht ein datenschutzrechtliches Problem darin, dass Daten zunächst keinen Personenbezug aufweisen mögen, aufgrund umfangreicher Verkettungen und hieraus resultierendem Zusatzwissen der jeweils verantwortlichen Stelle aber des Öfteren im Nachhinein ein Personenbezug hergestellt werden kann (zeitliche Komponente des Personenbezugs). Sobald ein solcher zu bejahen ist, finden dann die jeweils einschlägigen datenschutzrechtlichen Vorschriften Anwendung. [Roßnagel/Scholz 2000] weisen in diesem Zusammenhang auf die Notwendigkeit von Vorsorgeregelungen hin für den Fall, dass anonyme oder pseudonyme Daten im Nachhinein einen Personenbezug erhalten, und fordern entsprechende gesetzliche Regelungen, die die wenigen bisher vorhandenen Vorschriften[52] ergänzen sollen.

2.3.3.1.4 Verbot mit Erlaubnisvorbehalt

Wie bereits ausgeführt, kann eine Verknüpfung personenbezogener Daten entweder ein Verändern oder ein Nutzen der jeweiligen Daten darstellen, weshalb Gleiches auch für den inhaltsgleichen Begriff der Verkettung gilt.

Ob ein Verändern oder ein Nutzen von Daten vorliegt, spielt letztlich aber keine Rolle, weil in beiden Fällen das sog. Verbot mit Erlaubnisvorbehalt greift[53]. Nach diesem elementaren Prinzip des Datenschutzrechts ist jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn sie durch eine Rechtsvorschrift erlaubt oder angeordnet wird oder der Betroffene eingewilligt hat.

Bei jeder Verkettung von Daten ist also im Einzelfall zu prüfen, ob eine informierte und freiwillige Einwilligung oder eine Rechtsvorschrift die Verkettung legitimiert.

2.3.3.1.5 Zweckbindungsgrundsatz

Ein weiterer fundamentaler Grundsatz des Datenschutzrechts, der auch im Zusammenhang mit der Verkettung von Daten eine wichtige Rolle spielt, ist der sog. Zweckbindungsgrundsatz[54]. Nach diesem dürfen Daten nur zu bestimmten, vorher eindeutig bestimmten Zwecken verwendet werden. Eine Zweckänderung ist grundsätzlich verboten und nur in bestimmten Ausnahmefällen – etwa bei einer Einwilligung des Betroffenen in die Änderung – erlaubt. Ein Erlaubnistatbestand, der eine Datenverarbeitung zu einem bestimmten Zweck legitimiert, kann also nach dem Zweckbindungsgrundsatz nicht herangezogen werden, um auch eine beliebige Verkettung der jeweiligen Daten zu rechtfertigen.

2.3.3.1.6 Verkettung als juristischer Terminus

Die geltenden Datenschutzgesetze geben keine Begriffsdefinitionen für den Vorgang der Verkettung bzw. den Zustand der Verkettbarkeit vor. Im Volkszählungsurteil und in der Literatur findet sich vereinzelt der Begriff der Verknüpfung, wohingegen sich im Technikumfeld und unter einigen technikaffinen Juristen der Terminus Verkettung etabliert hat.

Insofern stellt sich die Frage, ob es für Juristen und Techniker nicht sinnvoll wäre, sich auf einen der beiden Begriffe, die das Gleiche bezeichnen, zu verständigen[55]. Hierfür spricht, dass eine effektive Zusammenarbeit dieser beiden Professionen im Datenschutzkontext heutzutage unabdingbar ist, weil ein wesentliches Ziel des modernen Datenschutzes darin besteht, bereits bei der Entwicklung von

[51] [Gola/Schomerus 2005, § 3 Rn. 9].

[52] Exemplarisch sei hier § 13 Abs. 7 TMG genannt, der den Nutzern von Telemedien einen Auskunftsanspruch gewährt, der sich auch auf die zu einem – eventuellen – Pseudonym gespeicherten Daten erstreckt.

[53] Dieses Verbot gehört zu den prägenden Grundsätzen des Datenschutzrechts und findet sich einfachgesetzlich etwa in §§ 4 Abs. 1 BDSG, 11 Abs. 1 LDSG SH oder 12 Abs. 1 TMG.

[54] Hierzu siehe etwa Weichert in [Däubler et al. 2007, Einl. Rn. 15] und [Tinnefeld/Ehmann/Gerling 2005, S. 150].

[55] Da das Gesetz keinen Begriff vorgibt, wären auch die Juristen insoweit frei darin, sich für einen der beiden Begriffe zu entscheiden.

Technik Einfluss auf deren Gestaltung zu nehmen („Datenschutz durch Technik“)[56]. Eine produktive Zusammenarbeit wird nun aber durch gemeinsame Begriffe und den zugrundeliegenden Konzepten deutlich erleichtert.

Dabei lässt sich für den Begriff der Verkettung anführen, dass er als gut geeignet dazu erscheint, als ein spezieller Datenschutz-Terminus auch in der breiteren Öffentlichkeit wahrgenommen zu werden. Hingegen wird der Begriff der Verknüpfung ebenso wie der auch noch in Betracht kommende Terminus der Vernetzung bereits in unterschiedlichen Kontexten verwendet.

2.3.3.1.7 Fazit

Eine Verkettung personenbezogener Daten ist zulässig, wenn die von der Verkettung betroffene Person zuvor ihre Einwilligung erteilt hat oder eine Rechtsvorschrift die Verkettung erlaubt. Des Weiteren ist insbesondere der Grundsatz der Zweckbindung zu beachten.

Aufgrund der Relativität und der zeitlichen Komponente des Personenbezugs können ursprünglich keinen Personenbezug aufweisende Daten zu einem späteren Zeitpunkt und/oder im Hinblick auf eine andere verantwortliche Stelle unvermittelt zu personenbezogenen Daten werden.

Es erscheint als sinnvoll, auf einen gemeinsamen Begriff von Technikern und Juristen für den Vorgang der Verkettung/Verknüpfung hinzuwirken.

2.3.3.2 Entkettungsmöglichkeiten aus der Sicht des Rechts

2.3.3.2.1 Einführung

Einmal miteinander verkettete Daten lassen sich grundsätzlich auch wieder entketten – zumindest ist dies rechtlich so vorgesehen[57]. Vorliegend wird der Begriff der Entkettung in einem weiten Sinne verstanden. Hiernach sind in diesem Zusammenhang insbesondere die folgenden Konstellationen zu unterscheiden:

- Zu einer Entkettung kommt es zunächst einmal dann, wenn (personenbezogene) Datenbestände zu verschiedenen Teilidentitäten oder verschiedene Daten zu einer (Teil-)Identität, die miteinander verkettet worden sind, wieder voneinander separiert werden. In diesen Fällen wird also die Verbindung, die zwischen zwei oder mehreren digitalen Teilidentitäten oder sonstigen Daten zu einer Person hergestellt worden ist, im Nachhinein wieder gelöst. Von Bedeutung ist in diesen Fällen oft, dass nicht nur die Zusammenführung der Daten wieder rückgängig gemacht werden muss, sondern auch Erkenntnisse, die durch die Verkettung gewonnen worden sind, nicht mehr berücksichtigt werden dürfen. Diese Problematik soll nachfolgend noch am Beispiel der Beweisverwertungsverbote des Strafprozessrechts und der verschiedenen Diskriminierungsverbote des Allgemeinen Gleichbehandlungsgesetzes (AGG) verdeutlicht werden[58].
- Werden ursprünglich personenbezogene Daten anonymisiert oder pseudonymisiert, so stellt dies einen speziellen Fall der Entkettung dar. Hier wird die Zuordenbarkeit von Daten zu einer bestimmten oder bestimmbaren Person – für alle oder zumindest für einen bestimmten Personenkreis – nachträglich beseitigt. Auf diese Thematik wird im Abschnitt 2.3.3.3 zu nutzergesteuerter Verkettung näher eingegangen.
- Schließlich wird hier auch jedes – vollständige oder teilweise – Löschen bzw. Sperren personenbezogener Daten unter den Begriff der Entkettung subsumiert. Deshalb soll in der Folge zunächst geschildert werden, unter welchen Voraussetzungen Daten nach dem BDSG zu löschen bzw. zu sperren sind. Vorgestellt werden sollen in diesem Kontext auch einige

[56] Einzelheiten hierzu finden sich bei [Roßnagel/Pfitzmann/Garstka 2001].

[57] In technischer Hinsicht wird dies indes in vielen Fällen zumindest schwierig, wenn nicht gar unmöglich sein (vgl. Abschnitt 4.10).

[58] In diesen Konstellationen geht es insbesondere auch um das psychologische Problem des „Vergessen-Müssens“.

wichtige gesetzliche Aufbewahrungspflichten, aufgrund derer eine Löschung von Daten erst nach Ablauf einer bestimmten Zeitspanne möglich ist.

2.3.3.2.2 Entkettung durch Löschen bzw. Sperren von Daten

2.3.3.2.2.1 Löschung personenbezogener Daten

Eine Entkettung kann zunächst durch die Löschung[59] – eines Teils – der personenbezogenen Daten erfolgen. Dabei ist zwischen der Erlaubnis und der Verpflichtung zur Löschung der Daten zu differenzieren. Nach § 35 Abs. 2 Satz 1 BDSG, der für den Bereich der Privatwirtschaft einschlägig ist[60], darf die jeweilige verantwortliche Stelle personenbezogene Daten grundsätzlich[61] jederzeit löschen. Eine Verpflichtung zur Löschung besteht nach Satz 2 der genannten Vorschrift dann, wenn

- die Speicherung der Daten unzulässig ist,
- es sich um besondere personenbezogene Daten wie solche über strafbare Handlungen, die Gesundheit oder das Sexualleben handelt und die verantwortliche Stelle deren Richtigkeit nicht beweisen kann,
- Daten für eigene Zwecke verarbeitet werden und ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist oder
- wenn die Daten – etwa von Auskunfteien – geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine alle vier Jahre vorzunehmende Prüfung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

Im Übrigen korrespondiert der Pflicht der verantwortlichen Stelle zur Löschung stets ein Anspruch des Betroffenen hierauf[62]. Nach § 6 Abs. 1 BDSG darf dieses Recht weder durch Rechtsgeschäft noch durch Betriebs- bzw. Dienstvereinbarung ausgeschlossen werden.

2.3.3.2.2.2 Sperrung personenbezogener Daten

2.3.3.2.2.2.1 Allgemeines

Der Begriff des Sperrens wird in § 3 Abs. 4 S. 2 Nr. 4 legaldefiniert als das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.

§ 35 Abs. 3 BDSG regelt die Fälle, in denen Daten trotz grundsätzlich bestehender Löschungspflichten weiter gespeichert werden dürfen bzw. müssen – in diesen Fällen tritt die Sperrung der Daten an die Stelle der Löschung. Dies gilt nach der genannten Vorschrift dann, wenn

- die Speicherung von für eigene Zwecke gespeicherten Daten nicht mehr erforderlich ist, einer Löschung aber gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten entgegenstehen[63],
- Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

---

59 Löschen wird in § 3 Abs. 4 S. 2 Nr. 5 definiert als das Unkenntlich-Machen gespeicherter personenbezogener Daten.

60 § 20 Abs.2 BDSG und die einschlägigen Vorschriften der Landesdatenschutzgesetze (vgl. etwa § 28 Abs. 2 LDSG SH) enthalten die für die Verwaltung einschlägigen Regelungen. Nachfolgend werden nur die für die Privatwirtschaft einschlägigen Vorschriften des BDSG hinsichtlich Löschung und Sperrung aufgeführt.

61 Dies gilt gem. § 35 Abs. 2 S. 1 i.V.m. Abs. 3 Nr. 1 und 2 BDSG ausnahmsweise nicht, wenn gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten einzuhalten sind oder die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigen würde. In diesen Fällen können die Daten lediglich gesperrt werden.

62 Hierzu siehe etwa Dix in [Simitis 2006, § 35 Rn. 1 f.].

63 Einen Überblick über die verschiedenen Aufbewahrungspflichten gibt Dix in [Simitis 2006, § 33 Rn. 66 ff.].

- eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Schließlich sind personenbezogene Daten auch zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

2.3.3.2.2.2.2 Wichtige gesetzliche Aufbewahrungspflichten

Relevante gesetzliche Aufbewahrungspflichten finden sich insbesondere im Handels- und im Steuerrecht:

§ 257 des Handelsgesetzbuchs (HGB) verpflichtet Kaufleute zur Aufbewahrung bestimmter Unterlagen. Hierzu gehören insbesondere

- Handelsbücher, Inventare, Eröffnungsbilanz, Jahresabschlüsse, Lageberichte sowie Konzernabschlüsse und -lageberichte und
- die empfangenen Handelsbriefe, d.h. alle Schriftstücke (hierunter fallen auch Telefaxe und E-Mails[64]), die ein Handelsgeschäft betreffen.

Hinsichtlich der Dauer der Aufbewahrungsfrist differenziert das Gesetz: Von den oben genannten Unterlagen sind die Handelsbriefe sechs Jahre, die übrigen Unterlagen zehn Jahre zu archivieren[65].

§ 147 der Abgabenordnung (AO) statuiert Aufbewahrungspflichten für Buchführungsunterlagen und ist von jedem Steuerpflichtigen, der buchführungs- oder aufzeichnungspflichtig ist, zu beachten. Aufzubewahren sind hiernach insbesondere

- Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte und Eröffnungsbilanzen,
- die empfangenen Handels- oder Geschäftsbriefe und Wiedergaben der versendeten Handels- oder Geschäftsbriefe,
- Buchungsbelege sowie
- sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind.

Auch hier differenziert das Gesetz bei der Dauer der Aufbewahrungsfrist: (Wiedergaben von) Handels- und Geschäftsbriefen und sonstige für die Besteuerung relevante Unterlagen sind sechs Jahre, die übrigen oben aufgelisteten Unterlagen hingegen zehn Jahre aufzubewahren[66].

2.3.3.2.3 Entkettung durch gezieltes Auflösen einer vorhandenen Verkettung

Wie bereits erwähnt, kann eine Entkettung auch durch ein gezieltes Beseitigen der Verbindung zwischen zwei oder mehreren digitalen Identitäten oder sonstigen (personenbezogenen) Daten herbeigeführt werden. In diesem Zusammenhang wird im Folgenden kurz auf juristische Regelungen, die eine (zumindest gedankliche) Entkettung von bereits zusammengeführten Informationen vorsehen, eingegangen: die Beweisverwertungsverbote des Strafprozessrechts und die Vorschriften des Allgemeinen Gleichbehandlungsgesetzes hinsichtlich einer Diskriminierung von Arbeitnehmern.

---

64 Siehe etwa Wiedmann in [Ebenroth/Boujong/Joost 2001, § 257 Rn. 15].

65 Dabei können mit Ausnahme der Eröffnungsbilanzen und Abschlüsse alle Unterlagen gem. § 257 Abs. 3 HGB auch als Wiedergabe auf einem Bildträger oder einem anderen Datenträger aufbewahrt werden, wenn hierbei bestimmten – vom Gesetz festgelegten – Anforderungen genügt wird.

66 Zu beachten ist insoweit, dass die Frist gem. § 147 Abs. 3 S. 3 AO so lange nicht abläuft, soweit und solange die Unterlagen für Steuern von Bedeutung sind, für die die Festsetzungsfrist noch nicht abgelaufen ist (sog. Ablaufhemmung).

2.3.3.2.3.1 Strafprozessuale Beweisverwertungsverbote

Ziel eines jeden Strafverfahrens ist die Erforschung der materiellen Wahrheit. Hierzu werden Beweise[67] erhoben, verwertet und gewürdigt. Allerdings darf die Wahrheit nicht um jeden Preis ermittelt werden[68], weshalb in bestimmten Konstellationen Beweisverbote einschlägig sind, die eine Erhebung bzw. Verwertung von Beweisen untersagen. Diese können sich nicht nur aus der Strafprozessordnung oder anderen gesetzlichen Regelungen, sondern auch unmittelbar aus dem Grundgesetz ergeben[69]. Bei den Beweisverboten können Beweiserhebungs- und Beweisverwertungsverbote unterschieden werden: Erstere erklären die Formen der Beweiserhebung für unzulässig, während Letztere eine Berücksichtigung bereits erhobener Beweise im Rahmen der Beweiswürdigung und der Urteilsfindung verbieten.

Hinsichtlich der hier näher zu betrachtenden Beweisverwertungsverbote[70] ist nun wiederum zwischen selbstständigen und unselbstständigen Verwertungsverboten zu differenzieren: Unter unselbstständigen Beweisverwertungsverboten sind solche zu verstehen, die sich aus einem Verstoß gegen ein Beweiserhebungsverbot ergeben. Hier ist allerdings zu beachten, dass eine fehlerhafte Beweiserhebung nicht zwangsläufig ein Beweisverwertungsverbot zur Folge hat. War die Beweiserhebung hingegen rechtmäßig, darf das Beweisergebnis aber dennoch nicht verwertet werden, so spricht man von einem selbstständigen Beweisverwertungsverbot.

Ist ein Beweisverwertungsverbot einschlägig, so darf das Gericht die im Rahmen der Beweiserhebung erlangten Informationen nicht in seine Erwägungen mit einbeziehen, es ist also gegebenenfalls dazu gezwungen, Informationen, die bereits Eingang in seine Überlegungen gefunden haben, wieder zu „vergessen“ und damit von anderen Informationen zu entketten. Werden also beispielsweise dem Beschuldigten gegenüber verbotene Vernehmungsmethoden wie Misshandlung, Ermüdung, Quälerei, Täuschung oder Hypnose eingesetzt, so darf eine Aussage des Beschuldigten, die insoweit zustande gekommen ist, nach § 136a Abs. 3 Satz 2 StPO nicht verwertet werden. Dies gilt selbst dann, wenn dieser der Verwertung zustimmt. Hat das Gericht eine Aussage bereits in seine Überlegungen mit einbezogen, stellt sich im Laufe der Hauptverhandlung aber heraus, dass diese unter Einsatz verbotener Vernehmungsmethoden zustande gekommen ist, so ist das Gericht also dazu gezwungen, diese Aussage von anderweitig erhobenen Beweisen zu entketten.

2.3.3.2.3.2 Diskriminierungsverbote des Allgemeinen Gleichbehandlungsgesetzes

Das Allgemeine Gleichbehandlungsgesetz (AGG) setzt vier Antidiskriminierungsrichtlinien der Europäischen Union um und ist im August 2006 in Kraft getreten. Ein wesentlicher Bestandteil des Gesetzes sind die in seinem zweiten Abschnitt (§§ 6 ff.) zu findenden Regelungen zum Schutz von Beschäftigten. Nach § 7 Abs. 1 AGG dürfen Beschäftigte – zu diesen zählen auch Personen, die sich auf eine Stelle hin bewerben – nicht wegen

- ihrer Rasse oder ethnischen Herkunft,
- ihres Geschlechts,
- ihrer Religion oder Weltanschauung,
- einer Behinderung,
- ihres Alters oder
- ihrer sexuellen Identität

benachteiligt werden.

---

[67] Beweismittel des Strafverfahrens sind in erster Linie Zeugen, Sachverständige und Augenschein sowie Urkunden und andere Schriftstücke.

[68] Vgl. BGHSt 14, 358 = NJW 1960, 1580; 31, 304 = NJW 1983, 1570 = NStZ 1983, 467.

[69] Hierzu vgl. etwa [Meyer-Goßner 2005, Einl. Rn. 56].

[70] Nähere Ausführungen hierzu finden sich etwa bei Pfeiffer in [Pfeiffer 2003].

Hieraus resultiert, dass der Arbeitgeber Informationen über einen oder mehrere der genannten Aspekte bei seinen Entscheidungen nicht – zum Nachteil für den Beschäftigten – berücksichtigen darf. Verfügt er über solche Informationen, so ist er dazu verpflichtet, diese von den anderen für seine Entscheidung maßgeblichen Umständen zu entketten. Dies soll nachfolgend am Beispiel des Bewerbungsverfahrens verdeutlicht werden[71].

Gemäß § 6 Abs. 1 Satz 2 AGG gelten die Vorschriften des Allgemeinen Gleichbehandlungsgesetzes auch für Personen, die sich auf eine freie Stelle hin bewerben. In diesem Zusammenhang muss ein Arbeitgeber zunächst beachten, dass ein Arbeitsplatz nicht unter Verstoß gegen das Benachteiligungsverbot des § 7 AGG ausgeschrieben werden darf[72]. Beispielsweise könnte schon das Verlangen eines Lichtbildes eine Diskriminierung darstellen, da dieses jedenfalls Aufschluss über Rasse, ethnische Herkunft, Geschlecht und Alter geben kann. Bedenkt man, dass etwa in den Vereinigten Staaten häufig Bewerbungen ohne Lichtbild, ohne oder mit abgekürztem Vornamen und ohne Alters- sowie Geschlechtsangabe eingereicht werden[73], erscheint eine solche Interpretation des Gesetzes jedenfalls nicht als völlig ausgeschlossen. In diesem Falle müsste der Arbeitgeber also auf das Anfordern eines Fotos verzichten und darüber hinaus auch Maßnahmen treffen, um zu verhindern, dass ein dennoch übersandtes Foto von den für die Einstellung verantwortlichen Mitarbeitern in Augenschein genommen werden kann – konkret müssten Bewerbungsunterlagen also auf Fotos hin gesichtet werden, die dann von den Unterlagen entfernt werden müssten. In einem solchen Fall käme es also sogar zu einer physischen Form der Entkettung. Hält man das Verlangen eines vollständigen Lebenslaufs mit Bild hingegen nach wie vor für zulässig, so erhalten die für die Einstellung verantwortlichen Mitarbeiter Kenntnis von Eigenschaften des Bewerbers, die sie im Rahmen ihrer Entscheidungsfindung nicht zu seinem Nachteil berücksichtigen dürfen. Hier müssten die Entscheidungsträger also – wie auch das jeweilige Gericht bei den Beweisverwertungsverboten – bereits erlangte (Zusatz-)Informationen wieder „vergessen“. Damit geht es in diesem Zusammenhang wiederum um eine gedankliche Entkettung, durch die eine diskriminierungsfreie Entscheidung sicherzustellen ist.

2.3.3.3 Nutzergesteuerte Verkettung

2.3.3.3.1 Einführung

Wie bereits ausgeführt ist eine Verkettung personenbezogener Daten nur zulässig, wenn sie durch eine Einwilligung des Betroffenen oder eine Rechtsvorschrift legitimiert wird. Allerdings besteht aufgrund der heute verfügbaren technischen Möglichkeiten ein hohes Risiko, dass Verkettungen unter Missachtung dieser rechtlichen Vorgaben vorgenommen werden.

Dies gilt insbesondere für den Bereich des Internets, wo jeder einzelne Nutzer beim Surfen umfangreiche Datenspuren hinterlässt[74]. So lassen sich etwa anhand der von einer Person aufgerufenen Webseiten oder von Anfragen an Suchmaschinen umfassende Profile über die Interessen und Vorlieben der betreffenden Person erstellen. Datenschutzrechtliche Relevanz erhalten diese Daten spätestens dann, wenn sie der betreffenden Person anhand der ihr zugewiesenen IP-Adresse oder mittels umfangreicher Verkettungen und hierdurch generierten oder sonst vorhandenen Zusatzwissens zugeordnet werden können.

Aus Sicht des Datenschutzes erscheint es deshalb als erstrebenswert, wenn nicht sogar unentbehrlich, allen Internetnutzern auch in technischer Hinsicht die Möglichkeit zu bieten, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen. Dies lässt sich durch Tools realisieren, die dem Einzelnen ein selbstgesteuertes Identitätsmanagement[75] ermöglichen. Ein solches nutzergesteuertes Identitätsmanagement basiert insbesondere auf Anonymisierungs- und Pseudonymi-

[71] Ausführliche Anmerkungen zu den (möglichen) Auswirkungen des AGG auf den Bewerbungsprozess finden sich bei [Eckert 2006, S. 1991].

[72] § 11 AGG. Folglich sind freie Stellen beispielsweise in aller Regel geschlechtsneutral auszuschreiben und die Stellenanzeigen dürfen keine Diskriminierung im Hinblick auf das Alter enthalten („junges dynamisches Team“ etc.).

[73] [Eckert 2006, S. 1991].

[74] Ausführlich hierzu [Köhntopp/Köhntopp 2000] sowie [Golembiewski 2003].

sierungstechniken, weshalb nachfolgend Anonymität und Pseudonymität aus der Perspektive des Rechts dargestellt werden.

2.3.3.3.2 Anonymität

2.3.3.3.2.1 Allgemeines

Die einfachste und effektivste Möglichkeit, eine missbräuchliche Verkettung digitaler Identitäten oder sonstiger personenbezogener Daten zu unterbinden, besteht in einem anonymen Auftreten[76].

Der Begriff der anonymen[77] Daten bezeichnet nach allgemeinem Verständnis Einzelangaben über eine Person, die dieser jedoch von keinem anderen zugeordnet werden können[78]. Korrespondierend hierzu ist nach [Pfitzmann/Hansen 2007] unter Anonymität der Zustand zu verstehen, innerhalb einer Menge von Subjekten (Anonymitätsmenge) nicht identifizierbar zu sein. Dabei ist der Anonymitätsgrad umso stärker, je größer die Anonymitätsmenge ist und je weniger das Verhalten der Mitglieder dieser Gruppe sich unterscheidet.

2.3.3.3.2.2 Verfassungsrecht: Besteht ein Grundrecht auf Anonymität?

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts ist allgemein anerkannt, dass natürliche Personen ein Grundrecht auf informationelle Selbstbestimmung haben. Darüber hinaus gehen verschiedene Stimmen in der Datenschutzliteratur davon aus, dass neben diesem Grundrecht auch ein eigenständiges Grundrecht auf Anonymität existiert[79].

Hierbei werden verschiedene Ansätze[80] verfolgt, nach denen das Grundrecht auf Anonymität

- ein selbstverständlicher Bestandteil des Grundrechts auf informationelle Selbstbestimmung,
- ein notwendiges Element informationeller Privatheit,
- ein grundlegendes Prinzip einer freiheitlichen Kommunikationsverfassung oder
- im Allgemeinen Persönlichkeitsrecht zu verorten ist.

Das Bundesverfassungsgericht hat sich allerdings noch nicht zu der Frage geäußert, ob ein allgemeines Grundrecht auf Anonymität existiert, des Weiteren ist dieses Thema auch in der verfassungsrechtlichen Literatur bisher kaum behandelt worden. Deshalb kann gegenwärtig (noch) nicht von einem allgemeinen Konsens in der Rechtswissenschaft gesprochen werden, dass ein solches allgemeines Grundrecht auf Anonymität existiert.

Jedenfalls wird ein anonymes Auftreten aber wie jegliches sonstiges Handeln durch das sog. Auffanggrundrecht der allgemeinen Handlungsfreiheit des Art. 2 I GG geschützt. Pauschal gesagt ist ein anonymes Auftreten danach solange zulässig, wie der Grundrechtsträger nicht gesetzlich zur Offenlegung seiner Identität verpflichtet ist[81].

---

75 Hierzu vgl. Abschnitt 4.6 zu nutzergesteuertem Identitätsmanagement in dieser Arbeit. Umfassende Ausführungen zum Thema Identitätsmanagement sowie ein Vergleich existierender Ansätze finden sich in [IMS Study 2003] sowie in [Bauer/Meints/Hansen 2005].

76 Im Internet wird ein solches anonymes Auftreten durch Tools wie den Anonymisierungsdienst AN.ON mit der Software JAP ermöglicht. Einzelheiten zu diesem und weiteren sog. Anonymizern folgen im Abschnitt 4.5.1.

77 Der Begriff anonym kommt aus dem Griechischen und bedeutet soviel wie „namenlos“ oder „namentlich unbekannt“.

78 [Roßnagel/Scholz 2000, S. 723].

79 In den einschlägigen Kommentaren und Lehrbüchern des Staats- und Verfassungsrechts sowie des Medien- und Kommunikationsrechts finden sich erstaunlicher Weise hingegen so gut wie keine Ausführungen zu diesem Thema.

80 Ausführlich hierzu [Mutius 2003].

81 Natürlich kann eine Person auch faktisch zur Offenbarung ihrer Identität gezwungen sein, wenn sie etwa mit einem bestimmten Vertragspartner kontrahieren möchte und dieser nur unter dieser Voraussetzung hierzu bereit ist. Zum Thema Identifizierungspflichten siehe auch den Abschnitt 3.2.1.3.

2.3.3.3.2.3 Einfachgesetzliche Regelungen

Auf einfachgesetzlicher Ebene gibt es mittlerweile verschiedene Regelungen, die das Thema Anonymität betreffen. Die wichtigsten Vorschriften finden sich im Bundesdatenschutzgesetz (BDSG) und im Telemediengesetz[82] (TMG):

So statuiert § 3a BDSG den Grundsatz der Datenvermeidung und -sparsamkeit[83], wonach sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten haben, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Zu diesem Zweck ist der genannten Vorschrift zufolge insbesondere, von der Möglichkeit der Anonymisierung[84] Gebrauch zu machen. Dabei bezeichnet der Begriff des Anonymisierens im Sinne des BDSG das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können[85]. Allerdings muss eine Anonymisierung nur erfolgen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht[86].

Eine Konkretisierung des Grundsatzes der Datenvermeidung und -sparsamkeit findet sich in § 40 BDSG. Nach dieser Vorschrift sind Daten, die für Zwecke der wissenschaftlichen Forschung erhoben oder gespeichert worden sind, zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist[87].

Während § 3a BDSG also primär auf eine nachträgliche Anonymisierung von zunächst personenbezogenen Daten abzielt, geht das Telemediengesetz einen Schritt weiter: Gemäß § 13 Abs. 6 TMG haben Diensteanbieter u.a. die anonyme Nutzung von Telemedien[88] und ihre Bezahlung zu ermöglichen, soweit dies technisch möglich und zulässig ist. Der Nutzer ist über diese Möglichkeit zu informieren.

Die genannte Vorschrift möchte es den Nutzern von Telemedien also ermöglichen, von vornherein zu vermeiden, dass personenbezogene Daten überhaupt entstehen. Nach [Bäumler 2003, S. 5] kann aus ihr ein Recht des Nutzers auf anonyme Inanspruchnahme von Diensten abgeleitet werden[89]. Zwar sind primäre Adressaten der Vorschrift nicht die Nutzer, sondern die Diensteanbieter; für die Bejahung eines Rechts auf anonyme Inanspruchnahme solcher Dienste spricht aber nicht zuletzt der Umstand, dass die Nutzer über die Möglichkeit einer anonymen Nutzung zu informieren sind.

Unabhängig hiervon hat der Gesetzgeber mit dem Erlass dieser Vorschrift die grundlegende Entscheidung für Anonymität im Internet, die sich bereits den durch das Telemediengesetz abgelösten Vorschriften des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrags entnehmen ließ, erneut bestätigt[90]. Jedoch steht auch das einfachgesetzliche Recht auf Anonymität des § 13 Abs. 6 TMG unter dem Vorbehalt, dass eine anonyme Nutzung technisch möglich und zumutbar ist[91].

---

82 Dieses Gesetz ist am 01.03.2007 in Kraft getreten und hat das Teledienstegesetz (TDG), das Teledienstedatenschutzgesetz (TDDSG) und den Mediendienste-Staatsvertrag (MDStV) abgelöst. Hinsichtlich der Möglichkeit einer anonymen Nutzung von Telemedien hat sich durch den Erlass des TMG nichts geändert, da bereits das TDDSG und der MDStV inhaltsgleiche Vorschriften enthielten.

83 Dieser findet sich ebenfalls in den Landesdatenschutzgesetzen (vgl. z.B. § 4 Abs. 1 LDSG SH), aber auch etwa in den Datenschutzregelungen des Sozialrechts (vgl. § 78b S. 1 SGB X).

84 Gleiches gilt für die Möglichkeit der Pseudonymisierung, auf die weiter unten eingegangen werden wird.

85 Siehe die Legaldefinition des § 3 Abs. 6 BDSG.

86 Entscheidend ist hier das Kriterium der Zumutbarkeit: Dabei hängt es jeweils von den Umständen des Einzelfalles ab, welcher Aufwand noch als zumutbar angesehen werden kann. Zu berücksichtigen sind hier insbesondere die voraussichtlich anfallenden Kosten und die Leistungsfähigkeit der jeweiligen verantwortlichen Stelle.

87 § 40 Abs. 2 S. 1 BDSG.

88 Der Begriff Telemedien umfasst alle elektronischen IuK-Dienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 Telekommunikationsgesetz (TKG), die ganz in der Übertragung von Signalen bestehen, oder Rundfunk im Sinne von § 2 Rundfunkstaatsvertrag (RStV) sind.

89 Diese Aussage bezog sich zwar noch auf die Regelung in § 4 Abs. 6 TDDSG, kann aber ohne weiteres auf die inhaltsgleiche Vorschrift des § 13 Abs. 6 TMG übertragen werden.

90 Es ist aber anzumerken, dass die künftigen gesetzlichen Regelungen zur sog. Vorratsdatenspeicherung sich hiermit wohl nur schwer vereinbaren lassen werden.

91 Mit der Frage, wann eine Zumutbarkeit zu bejahen ist, beschäftigen sich ausführlich [Fritsch et al. 2005].

2.3.3.3.2.4 Anwendbarkeit der Datenschutzgesetze

Werden anonymisierte bzw. bereits von Anfang an anonyme Daten verwendet, so lässt sich die Möglichkeit einer Re-Identifizierung dennoch niemals vollständig ausschließen[92]. Nach der Legaldefinition des § 3 Abs. 6 BDSG liegt ein Anonymisieren vor, wenn Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großem Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Ist die Wahrscheinlichkeit einer Re-Identifizierung anonymer Daten mithin so gering, dass sie nach der Lebenserfahrung oder der wissenschaftlichen Prognose praktisch ausscheidet, so sind die Datenschutzgesetze nach [Roßnagel/Scholz 2000] mangels eines Personenbezugs dieser Daten nicht anwendbar. Dammann in [Simitis 2006, § 3 Rn. 196] unterscheidet hingegen zwischen „faktisch" anonymisierten Daten, bei denen der Personenbezug – wenn auch nur mit unverhältnismäßig großem Aufwand – noch wiederhergestellt werden kann und „absolut" anonymisierten Daten, bei denen eine Zuordnung nicht mehr möglich ist. Nur bei Letzteren sollen hiernach nach dem Anonymisierungsvorgang keine personenbezogenen Daten mehr vorliegen.

2.3.3.3.3 Pseudonymität

2.3.3.3.3.1 Allgemeines

Anonymität ist zwar ein gut geeigneter Weg zur Sicherstellung von Datenvermeidung und Datensparsamkeit sowie zur Verhinderung ungewollter Verkettungen von Daten. Ein anonymes Auftreten ist aber nicht immer möglich oder erwünscht. So wird sich etwa bei Rechtsgeschäften, bei denen eine Partei in Vorleistung tritt, diese regelmäßig nicht darauf einlassen, ihre Leistung gegenüber einer anonym handelnden Person zu erbringen. Vielmehr wird es für diese Partei meist von entscheidender Bedeutung sein, dass sie im Falle einer Nicht- oder Schlechtleistung des Vertragspartners ihre diesbezüglichen Ansprüche gegenüber diesem auch durchsetzen kann.

In solchen Situationen ist es nun aber nicht unbedingt erforderlich, dass der Vertragspartner seine Identität von Anfang an offenlegt. In vielen Fällen wird es vielmehr ausreichen, wenn die Identität des Vertragspartners im Konfliktfall aufgedeckt werden kann. An dieser Stelle kommt nun aber der Einsatz von Pseudonymen ins Spiel, deren Vorteil gegenüber einem anonymen Auftreten in der Möglichkeit besteht, die Identität des Pseudonymträgers bei Bedarf offenlegen zu können.

Begrifflich handelt es sich bei Pseudonymen[93] um Bezeichner für Subjekte, die von den realen Namen der jeweiligen Personen verschieden sind. Wie die folgenden Beispiele verdeutlichen, kommen als Pseudonyme höchst unterschiedliche Bezeichner in Betracht: Künstlername, Spitzname, Telefonnummer, Kontonummer, IP-Adresse, E-Mail-Adresse oder biometrische Daten wie Fingerabdruck oder digitales Gesichtsbild. Korrespondierend zum Begriff des Pseudonyms ist unter Pseudonymität die Nutzung von Pseudonymen als Bezeichner zu verstehen. Charakteristisch ist dabei das Bestehen einer Zuordnungsregel, anhand derer die jeweilige Person identifiziert werden kann. Pseudonymität umfasst folglich das gesamte Spektrum zwischen Anonymität und eindeutiger Identifizierbarkeit.

2.3.3.3.3.2 Verfassungsrecht

Auch die Verwendung von Pseudonymen und die hiermit verbundene Verschleierung der eigenen Identität wird – wie ein anonymes Auftreten – jedenfalls durch das Auffanggrundrecht der allgemeinen Handlungsfreiheit geschützt. Das Auftreten unter einer anderen Identität ist also wie jede sonstige menschliche Handlung auch als zulässiger Freiheitsgebrauch anzusehen, solange es nicht die Rechte anderer verletzt oder gegen das Sittengesetz oder die verfassungsmäßige Ordnung verstößt[94].

---

92 Vgl. etwa [Tinnefeld/Ehmann/Gerling 2005, S. 287].

93 Der Begriff „pseudonym" kommt wie „anonym" aus dem Griechischen und bedeutet soviel wie „fälschlicherweise so genannt".

94 Ausführlich hierzu [Krasemann 2006a]. Dieser vertritt darüber hinaus auch die Ansicht, dass die Verwendung von Pseudonymen auch vom Recht auf informationelle Selbstbestimmung getragen wird.

Ein zulässigerweise verwendetes Pseudonym kann auch verfassungsrechtlichen Schutz durch das allgemeine Persönlichkeitsrecht des Art. 2 I i.V.m. 1 I GG genießen[95].

2.3.3.3.3.3 Einfachgesetzliche Regelungen

Auf einfachgesetzlicher Ebene finden sich Regelungen zum Thema Pseudonymität[96] im Bundesdatenschutzgesetz und im Telemediengesetz. Darüber hinaus enthält beispielsweise auch das Signaturgesetz Vorschriften zur Verwendung von Pseudonymen.

Nach § 3a S. 2 BDSG ist zum Zwecke der Datenvermeidung und Datensparsamkeit auch von der Möglichkeit der Pseudonymisierung Gebrauch zu machen. Pseudonymisieren im Rechtssinne bedeutet das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können[97]. Von der Möglichkeit der Pseudonymisierung muss – analog zu der der Anonymisierung – dann Gebrauch gemacht werden, wenn dies technisch möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Nach § 40 BDSG müssen personenbezogene Daten, die für Zwecke der wissenschaftlichen Forschung verwendet werden, nicht nur anonymisiert werden, sobald dies nach dem Forschungszweck möglich ist. Die Vorschrift schreibt vielmehr auch eine pseudonymisierte Speicherung der Daten vor. Die Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, müssen gesondert gespeichert werden und dürfen mit den Einzelangaben nur dann zusammengeführt werden, wenn der Forschungszweck dies erfordert[98].

§ 13 Abs. 6 TMG räumt den Nutzern von Telemedien ein einfachgesetzliches Recht auf die Verwendung von Pseudonymen ein. Hiernach muss der Diensteanbieter neben der anonymen auch die pseudonyme Nutzung und Bezahlung von Telemedien ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist zudem über diese Möglichkeit zu informieren. Des Weiteren findet sich eine Regelung in § 13 Abs. 7 TMG, wonach ein Anbieter von Telediensten einem Nutzer auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen hat[99].

Weitere Vorschriften des Telemediengesetzes regeln die Voraussetzungen, unter denen dem Diensteanbieter die Erstellung von Nutzungsprofilen seiner Kunden gestattet ist. Hiernach dürfen solche Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien erstellt werden, sofern hierfür Pseudonyme verwendet werden und der Nutzer dem nicht widerspricht[100].

Konsequenterweise sieht das Gesetz außerdem vor, dass Daten über den Träger des jeweiligen Pseudonyms auch nachträglich nicht mit Nutzungsprofilen zusammengeführt werden dürfen[101]. Wer dies dennoch – vorsätzlich oder fahrlässig – tut, begeht eine Ordnungswidrigkeit, die mit einer Geldbuße von bis zu 50.000 EUR geahndet werden kann[102]. Um eine nachträgliche Zusammenführung

[95] Zuletzt bestätigt hat das Bundesverfassungsgericht dies in seinem Beschluss vom 21.09.2006 („Maxem“) = NJW 2007, 671: „Der verfassungsrechtlich durch das allgemeine Persönlichkeitsrecht gewährleistete Schutz des Namens erschöpft sich nicht im Schutz des bürgerlichen Namens. Auch der von einem Menschen tatsächlich geführte Name kann verfassungsrechtlichen Schutz genießen, wenn sich mit ihm eine Identität und Individualität des Namensträgers herausgebildet und verfestigt haben und auch herausbilden durften (vgl. BVerfG [3. Kammer des Ersten Senats], NJWE-FER 2001, 193 [194]). Diese Funktion kann auch ein Pseudonym übernehmen (vgl. BverfGE 78, 38 [52] = NJW 1988, 1577)." Im konkreten Fall sah das Gericht allerdings den Schutzbereich des allg. Persönlichkeitsrechts als nicht berührt an.

[96] Wie auch schon zur Anonymität.

[97] Diese dem § 2 Abs. 2 S. 2 Nr. 7 LDSG SH entnommene Definition ist prägnanter als die des § 3 BDSG, die das entscheidende Element der Zuordnungsregel überhaupt nicht erwähnt.

[98] § 40 Abs. 2 S. 2 und 3 BDSG.

[99] Diese Regelung ist lex specialis zum Auskunftsanspruch des § 34 BDSG.

[100] § 15 Abs. 3 S. 1 TMG.

[101] § 15 Abs. 3 S. 3 TMG.

[102] § 16 Abs. 2 Nr. 6, Abs. 3 TMG.

von Nutzungsprofilen und identifizierenden Angaben auch in tatsächlicher Hinsicht auszuschließen oder zumindest zu erschweren, wird der Diensteanbieter außerdem dazu verpflichtet, durch technische und organisatorische Vorkehrungen sicherzustellen, dass Nutzungsprofile nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können[103].

Das Signaturgesetz (SigG) enthält ebenfalls Regelungen, die die Verwendung von Pseudonymen betreffen – insbesondere ermöglicht es die Verwendung pseudonymer qualifizierter Signaturen[104]. Nach § 5 Abs. 3 Satz 1 SigG kann der Antragsteller nämlich vom Zertifizierungsdiensteanbieter verlangen, dass dieser in einem qualifizierten Zertifikat nicht den Namen des künftigen Signaturschlüssel-Inhabers, sondern ein Pseudonym aufführt. Dieses muss als solches erkennbar und unverwechselbar sein[105].

Gem. § 14 Abs. 2 Satz 1 SigG darf der Zertifizierungsdiensteanbieter die Identität eines pseudonymen Signaturschlüssel-Inhabers nur in wenigen Ausnahmefällen aufdecken. Pauschal gesagt ist eine Aufdeckung der Identität nach der Wertung des Signaturgesetzes dann rechtlich zulässig, wenn überwiegende Interessen der Allgemeinheit dies erfordern[106]. Außerdem darf die Aufdeckung nur dann erfolgen, wenn die jeweils zuständige Behörde hierum ersucht. Darüber hinaus ist jede Auskunftserteilung zu dokumentieren[107]. Schließlich ist die ersuchende Behörde dazu verpflichtet, den Signaturschlüssel-Inhaber über die Übermittlung der Identitätsdaten zu unterrichten[108]. Dies muss spätestens dann geschehen, wenn durch diese Unterrichtung die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird.

Anzumerken ist an dieser Stelle noch, dass es im Verwaltungsrecht verschiedene Rechtsnormen gibt, die die Verwendung pseudonymer Signaturen entweder kategorisch ausschließen oder nur dann gestatten, wenn das verwendete Pseudonym eine Identifizierung der Person des Signaturschlüssel-Inhabers ermöglicht[109]. Diese Regelungen spielen vor allem im E-Government-Kontext eine Rolle, wo sie die Möglichkeit einer Verwendung pseudonymer Signaturen erheblich einschränken[110].

2.3.3.3.3.4 Anwendbarkeit der Datenschutzgesetze

Die Anwendbarkeit der jeweils einschlägigen Datenschutzgesetze richtet sich wiederum danach, ob die pseudonymen Daten für die Daten verarbeitende Stelle einen Personenbezug aufweisen.

[Roßnagel/Scholz 2000] vertreten insoweit – wie auch hinsichtlich anonymer Daten – den Standpunkt, dass ein Personenbezug zu verneinen ist, wenn die Wahrscheinlichkeit, dass die verarbeitende Stelle die Daten einer bestimmten Person zuordnen kann, so gering ist, dass sie nach der Lebenserfahrung oder der wissenschaftlichen Prognose praktisch ausscheidet. Es ist also in jedem Einzelfall zu untersuchen, wie hoch die Wahrscheinlichkeit einer Aufdeckung des jeweiligen Pseudonyms ist. Ein solches kann zum einen dann aufgedeckt werden, wenn die Zuordnungsregel verfügbar ist, zum anderen dann, wenn das vorhandene Kontextwissen der Daten verarbeitenden Stelle die Aufdeckung ermöglicht.

Ein Pseudonym kann zunächst dann aufgedeckt werden, wenn die entsprechende Zuordnungsregel bekannt ist. Dabei kann die Daten verarbeitende Stelle von Anfang an Kenntnis von der Zuordnungsregel haben. Dies ist insbesondere dann der Fall, wenn sie das Pseudonym selbst vergibt. Sie kann aber auch erst später Kenntnis von der Zuordnungsregel erlangen, etwa wenn der Pseudonyminhaber das Pseudonym ihr gegenüber aufdeckt oder wenn sie die Zuordnungsregel von Dritten erfährt.

Wie jeder sonstige Personenbezug kann auch ein Bezug zwischen einem Pseudonym und dessen Inhaber mit Hilfe von Kontextwissen hergestellt werden. Generiert werden kann ein solches Kontext-

[103] § 13 Abs. 4 S. 1 Nr. 6 TMG.
[104] Ausführliche Ausführungen hierzu finden sich bei [Hopp/Grünvogel 2002].
[105] § 7 Abs. 1 Nr. 1 SigG.
[106] [Hopp/Grünvogel 2002, S. 80].
[107] § 14 Abs. 2 S. 2 SigG.
[108] § 14 Abs. 2 S. 3 SigG.
[109] Vgl. §§ 3a Abs. 2 S. 3 VwVfG, 36 a Abs. 2 S. 3 SGB I, 87 a Abs. 3 S. 3 AO.
[110] [Gundermann 2003] kommt zu dem Ergebnis, dass die Offenlegung der Identität in fast allen E-Government-Konstellationen unumgänglich ist, weshalb eine Verwendung von Pseudonymen in diesen Fällen ausscheidet. Hierzu später mehr im Abschnitt 3.2.5 zu E-Government im Status-Quo-Teil dieser Arbeit.

wissen insbesondere durch die Verkettung und Auswertung von Daten, die im Zusammenhang mit der Nutzung eines bestimmten Pseudonyms im Laufe der Zeit angefallen sind.

Anders als [Roßnagel/Scholz 2000] ist Bizer in [Simitis 2006, § 3 Rn. 217] der Meinung, dass pseudonymisierte Daten stets personenbeziehbare Daten im Sinne des § 3 Abs. 1 BDSG sind, wenn eine Zuordnungsregel besteht. Hiernach ist nicht „zwischen dem Personenkreis, der die Zuordnungsregel kennt ('innen'), und denjenigen, die sie nicht kennen ('außen')“, zu differenzieren.

2.3.4 Technische Grundlagen

Sollen Aktionen von Menschen in informationstechnisches Systeme (IT-Systeme) abgebildet werden, so haben der Akteur sowie seine möglichen Interakteure bestimmte Erwartungen, zu denen insbesondere auch Sicherheitsanforderungen gehören, die das IT-System für Aktionen gewährleisten soll. Dabei wird in der Regel eine Dreiteilung der Sicherheitsanforderungen vorgenommen (vgl. [Voydock/Kent 1983], [ZSI 1989]):

- Vertraulichkeitsanforderungen (engl.: „confidentiality requirements“): Unbefugter Informationsgewinn aus dem System soll verhindert werden.
- Integritätsanforderungen (engl.: „integrity requirements“): Unbefugte Modifikation von Information im System soll verhindert werden.
- Verfügbarkeitsanforderungen (engl.: „availability requirements“): Unbefugte Beeinträchtigung der Funktionalität des Systems soll verhindert werden.

Diese Dreiteilung muss für konkrete Systeme in Form konkreter Sicherheitsanforderungen weiter präzisiert werden.

2.3.4.1 Kommunikationssysteme

Kommunikationssysteme wurden auf auftretende Sicherheitsanforderungen der Beteiligten bereits ausführlich untersucht. Es vermittelt Kommunikation zwischen Kommunikationspartnern in Form von Nachrichten von Absendern zu Adressaten. Die im System auftretenden Informationen, auf die sich die Sicherheitsanforderungen Vertraulichkeit und Integrität beziehen, setzen sich aus Inhalt und Kommunikationsumständen der zugehörigen Nachricht zusammen. Unter Kommunikationsumstände fallen der zugehörige Absender und die Adressaten. Zusätzlich können die Kommunikationspartner weitere Umstände, die im Kommunikationssystem als Informationen auftreten, als schützenswert ansehen; dazu können beispielsweise die Zeit, zu der sie kommunizieren, oder der Ort, an dem sie sich befinden, zählen. Für Kommunikationssysteme lassen sich die drei obigen Anforderungen wie in der nachfolgenden Tabelle 5 zusammengefasst präzisieren:

Schutz der / mögliche Bedrohungen	Kommunikations-inhalte	Kommunikations-umstände
unautorisierter Zugriff auf Informationen → Vertraulichkeitsziele	Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
unautorisierte Modifikation von Informationen → Integritätsziele	Integrität Unstörbarkeit	Zurechenbarkeit[111] Abrechenbarkeit Datenkonsistenz
unautorisierte Beeinträchtigung der Nutzbarkeit → Verfügbarkeitsziele	Verfügbarkeit[112]	Erreichbarkeit[113] Verbindlichkeit Fairness[114]

Tabelle 5: Schutzziele in Kommunikationssystemen

1. Die Vertraulichkeitsanforderungen umfassen
   a) Anonymität (engl.: „anonymity“) des Absenders bzw. der Adressaten einer Nachricht, d.h., diese sind innerhalb einer Menge möglicher Absender bzw. Adressaten nicht identifizierbar („anonymity ist the state of being not identifiable within a set of subjects, the anonymity set“, vgl. [Pfitzmann/Hansen 2007]).
   b) Unbeobachtbarkeit (engl.: „unobservability“) des Absenders oder der Adressaten einer Nachricht, d.h., jemand kann Absender oder Adressat der Nachricht sein, ohne dass andere außer ihnen dies bemerken.
   c) Vertraulichkeit des Inhalts einer Nachricht, d.h., niemand außer dem Absender und den Adressaten einer Nachricht kennt deren Inhalt.
   d) Verdecktheit (engl.: „hiding“) des Inhalts einer Nachricht, d.h., niemand außer dem Absender und den Adressaten einer Nachricht bemerkt deren Existenz.
2. Die Integritätsanforderungen umfassen:
   a) Integrität des Inhalts und der Kommunikationsumstände einer Nachricht, d.h., niemand kann eine Nachricht nach deren Absenden unbemerkt modifizieren.
   b) Zurechenbarkeit (engl.: „accountability“) des Absenders bzw. der Adressaten einer Nachricht, d.h., ein Absender bzw. Adressat kann nicht erfolgreich abstreiten, eine Nachricht mit diesem Inhalt und den übermittelten Kommunikationsumständen gesendet bzw. erhalten zu haben.
   c) Datenkonsistenz (engl.: „data consistency“) des Inhalts und des Absenders einer Nachricht, d.h., alle Adressaten einer Nachricht erhalten die gleiche Nachricht mit dem gleichen Inhalt und den gleichen Kommunikationsumständen oder erkennen, dass dies nicht der Fall ist.
3. Die Verfügbarkeitsanforderungen umfassen:

a) Verfügbarkeit des Systems, das die Nachricht vermittelt, d.h., eine Entität kann eine Nachricht senden oder empfangen, wenn sie dies möchte.

b) Erreichbarkeit (engl.: „reachability“) der Entitäten innerhalb des Systems, d.h., Entitäten können über eine Nachricht erreicht werden oder auch nicht, abhängig von ihren Wünschen.

[111] Erhöht die Glaubwürdigkeit.
[112] Fördert QoS (Quality of Service).
[113] Muss vermutlich auf Anwesenheit (etwa in einer Gruppenkommunikation) erweitert werden.
[114] Fördert die Gleichberechtigung (der Kommunikationspartner).

c) Fairness (engl.: „fairness“) der Entitäten untereinander, d.h., alle Absender bzw. Adressaten haben die gleichen Möglichkeiten zum Senden bzw. Empfang einer Nachricht.

d) Verbindlichkeit (engl.: „legal enforceability“) der Entitäten, d.h., Entitäten können dafür verantwortlich gemacht werden, versprochenen Verpflichtungen nachzukommen.

Die Anforderungen 1(a)-(c), 2(a)-(b) sowie 3(a) wurden bereits in den Common Criteria [CC 1998] zusammengefasst. Diese Anforderungen wurden in [Wolf/Pfitzmann 2000] aufgegriffen und um die Anforderungen 1(d), 3(b) und 3(d) ergänzt. Alle Sicherheitsanforderungen sind immer gerichtet gegenüber anderen Entitäten, gegenüber denen sie gelten sollen. Welche Sicherheitsanforderungen gegenüber welchen anderen Entitäten gelten können, wird für alle Anforderungen außer (2c) und 3(c) ebenfalls in [Wolf/Pfitzmann 2000] näher ausgeführt. Da ein Kommunikationssystem in der Regel mehrere Absender und mehrere Empfänger haben kann – sonst wäre Anonymität der Absender ohne Unbeobachtbarkeit gar nicht möglich –, wurden 2(c) und 3(c) hier als weitere Sicherheitsanforderungen ergänzt.

Das letzte Ziel 3(d) – die Verbindlichkeit – befindet sich bereits außerhalb des technischen Systems, sondern muss – wie der englische Begriff dafür bereits sagt – juristisch behandelt werden. Verbindlichkeit hängt insbesondere davon ab, inwieweit die verwendeten technischen Maßnahmen zur Umsetzung der Sicherheitsanforderungen im geltenden Recht als ausreichend und rechtlich bindend angesehen werden. Der daraus oft folgende juristische Prozess ist meist teuer und aufwändig für denjenigen, der die Verpflichtung des anderen durchsetzen möchte, und sollte aus seiner Sicht vermieden werden. Umgekehrt sind mögliche rechtliche Konsequenzen für denjenigen, der sich entgegen seiner versprochenen Verpflichtung verhalten möchte, hoffentlich abschreckend genug, dies doch nicht zu tun.

2.3.4.2 Anforderungen in komplexeren IT-Systemen

In Kommunikationssystemen wurden nur Sicherheitsanforderungen bezüglich einer einzelnen Nachricht betrachtet. In vielen IT-Systemen (beispielsweise im E-Commerce) tritt jedoch nicht nur uni- oder bidirektionale Kommunikation auf, sondern es gibt auch Verkettungen von Aktionen in Form von Interaktionen oder von Aktionen derselben Person. Dies führt zu neuen Sicherheitsanforderungen:

- Mit der Anmeldung bei einem Dienst erhält ein Nutzer das Recht unter dem beim Eintritt vereinbarten Pseudonym Aktionen auszuführen (Pseudonymität („pseudonymity“) von Aktionen); mit der Abmeldung wird ihm dieses Recht entzogen. Dadurch nimmt der Nutzer abhängig von seinen Aktionen unter einem Pseudonym eine beliebige Zwischenstufe zwischen Anonymität und Identifizierbarkeit ein.
- Die Pseudonymverwendung samt geeigneter Authentisierung bzw. Identifizierungsmaßnahmen erlaubt Wiedererkennung für den Anbieter. Auf der Basis von Authentisierung eines Pseudonyms kann seine Autorisierbarkeit (engl.: „authorisability“) für Aktionen möglich ist. Die unter dem Community Pseudonym begangenen Aktionen sind diesem zurechenbar und der Inhaber soweit erforderlich aufdeckbar und haftbar.
- Durch Verkettbarkeit von Informationsflüssen bzw. den sich so ergebenden Aktionsfolgen kann unter Umständen nach verschiedenen Ausschlusskriterien die Menge der möglichen Akteure reduziert werden, was deren Anonymität gefährdet. Damit kann Unverkettbarkeit (engl.: „unlinkability“ gem. [Pfitzmann/Hansen 2007]) von Aktionen eine Sicherheitsanforderung von Akteuren sein.

In Kommunikationssystemen ist es üblich, dass sowohl Kommunikationspartner als auch nicht an der Kommunikation Beteiligte als potenzielle Angreifer gesehen werden können. Nach [Wolf/Pfitzmann 2000] müssen sich beide Kommunikationspartner über den Inhalt einer Nachricht betreffende Anforderungen (d.h. Vertraulichkeit, Verdecktheit, Integrität und Verfügbarkeit) einig sein, damit diese umgesetzt werden können, weshalb diese Anforderungen als gleichgerichtet bezeichnet werden.

Diese Anforderungen können mit technischen Maßnahmen allein nicht übergreifend garantiert werden; zusätzlich müssen die beteiligten Partner sie auf semantischer Ebene erfüllen. In Kommunikationssystemen, die Nachrichten zwischen sich vertrauenden Kommunikationspartnern

vermitteln, ist dies leichter zu erreichen als in IT-Systemen, wo Interaktionen zwischen einander noch unbekannten Entitäten entstehen können. Diese haben in Bezug auf die gleichgerichteten Sicherheitsanforderungen neben den Anforderungen an das IT-System auch Erwartungen an das Verhalten der Interakteure. Das IT-System soll nach Möglichkeit die Anforderungen sowohl auf technischer als auch auf semantischer Ebene garantieren (oder transparent machen, inwieweit dies geht bzw. nicht geht) [Borcea-Pfitzmann et al. 2007]:

1. Vertraulichkeit/Verdecktheit des Inhalts einer Aktion seitens des IT-Systems und der Interakteure soll bedeuten:
   a) Vertraulichkeit/Verdecktheit der Aktion im IT-System sowie
   b) Diskretion der Beteiligten bzgl. des Inhalts einer Aktion.
2. Integrität des Inhalts einer Aktion seitens des IT-Systems und der Interakteure soll bedeuten:
   a) Integrität der Aktion im IT-System sowie
   b) Korrektheit des durch einen Akteur erstellten Inhalts einer Aktion (bzw. dessen Handeln in gutem Glauben).
3. Verfügbarkeit des Inhalts einer Aktion seitens des IT-Systems und der Interakteure soll bedeuten:
   a) Verfügbarkeit des IT-Systems sowie
   b) Aktionsbereitschaft eines Akteurs zur Durchführung der gewünschten Aktion.

2.3.5 Ökonomische Grundlagen

2.3.5.1 Einleitung

Mit der Weiterentwicklung des Marketings in Richtung immer ausgefeilterer Marktforschungsinstrumente sind die Begehrlichkeiten an detaillierten Kundendaten gestiegen. Reichten früher die Adressdaten von Kunden und potenziellen Kunden aus, um den Unternehmenserfolg über Werbung zu steigern, wird heutzutage eine umfangreiche Datensammlung für die Unternehmenskommunikation betrieben. Mit Methoden der Marktforschung werden die Theorien und Modelle der Absatzmärkte empirisch überprüft und entsprechend angepasst, um den eigenen Verkaufserfolg zu erklären und zu steigern.

Die Entstehung des Internets mit seinen neuen Kommunikationsmöglichkeiten wie E-Mail, Diskussionsforen, Online-Shops und Blogs führt zu gesellschaftlichen Veränderungen, die die Erfassung von persönlichen Daten begünstigen. Für einen Großteil der Gesellschaft gehört dieses neue Medium beruflich und privat zum Leben dazu. Es ist heutzutage Bestandteil des Lifestyles, sich auch in der Online-Welt zu präsentieren. Die Anzahl der Geschäftsmodelle, die sich im Bereich Internet mit der Darstellung und Gestaltung von digitalen Identitäten beschäftigen, steigt: Internetservices wie z.B. Xing[115], StudiVZ[116], stayfriends[117] oder friendscout24[118] unterstützen den Nutzer bei dem strukturierten Aufbau einer digitalen Identität. Dem Trend folgend, dass immer mehr Lebensbereiche „online“ gehen, wird auch das Interesse an digitalen Identitäten steigen.

Digitale Identitäten stellen in einer Marktwirtschaft ein Wirtschaftsgut dar. Sie sind ein Rohstoff für das Marketing und die Unternehmen, die sich mit der Verkettung von Identitäten und der Aufbereitung dieser Daten beschäftigen. Im Folgenden werden die ökonomischen Aspekte zu Identitäten und deren Verkettung beleuchtet.

[115] http://www.xing.com/, Businesskontakt-Portal, ehemals openBC (letzter Zugriff im Oktober 2007).
[116] http://www.studivz.net/, „Studiverzeichnis“ (letzter Zugriff im Oktober 2007).
[117] http://www.stayfriends.de/, „Freunde-Suchmaschine“ (letzter Zugriff im Oktober 2007).
[118] http://www.friendscout24.de/, Online-Partnersuche (letzter Zugriff im Oktober 2007).

2.3.5.2 Der Wert von digitalen Identitäten

Die Preisbildung für ein Wirtschaftsgut erfolgt in einer Marktwirtschaft zumeist über die Wechselwirkung von Angebot und Nachfrage. Diese Preisbildung wird jedoch erschwert, wenn das Wirtschaftsgut nicht an transparenten Märkten gehandelt wird oder die Preisbildung durch gesetzliche Vorgaben eingeschränkt wird.

Betrachtet man die Wertschöpfungskette bei digitalen Identitäten, dann sind hier im Gegensatz zu anderen Wirtschaftsprozessen einige Besonderheiten zu beobachten. Die Wertschöpfungskette von digitalen Identitäten kann man vereinfacht durch den Ablauf beschreiben, der in Abbildung 4 dargestellt wird.

Abbildung 4: Wertschöpfungskette bei digitalen Identitäten

In dieser Darstellung der Wertschöpfungskette kann man zwei Teilmärkte feststellen: Auf Teilmarkt (a) werden Identitätsdaten unmittelbar von Privatpersonen oder gewonnen aus Beobachtungen von Firmen zur Verfügung gestellt und diese von Unternehmen genutzt/nachgefragt. Auf dem Teilmarkt (b) werden Identitäten in unterschiedlichen Aufbereitungsgraden angeboten und von Unternehmen, die mit diesen Daten ihren Unternehmenserfolg steigern möchten, nachgefragt.

Die beiden Teilmärkte folgen hierbei ganz unterschiedlichen Regeln. Der Teilmarkt (b) bildet seinen Preis für die Ware „digitale Identitäten“ durch Angebot und Nachfrage. Für die beteiligten Marktteilnehmer sind die Kosten und der Nutzen relativ klar zu bewerten. Der Anbieter hat Kosten für die Beschaffung des Ausgangsstoffes, in diesem Fall die digitalen Identitäten, und den daran anschließenden Produktionsprozess, in dem die Identitäten verkettet und aufbereitet werden. In dem Verkaufspreis werden sich die Aktualität, die Qualität, der Umfang der Verkettung, die Exklusivität und der Intimitätsgrad des Datenmaterials widerspiegeln. Der Nachfrager kann den Nutzen für den Einsatz der digitalen Identitäten quantifizieren, indem er beispielsweise die möglichen Steigerungen von Umsatz bzw. Gewinn oder die Einsparungen im Marketing durch geringere Streuverluste den Kosten für den Erwerb der Identitäten gegenüberstellt.

Diese Nutzenkalküle dürften auf dem Teilmarkt (a) nicht so klar ausgeprägt sein, so dass die Preisbildung – wenn überhaupt – nur wenig transparent erfolgt. Es scheint, dass viele Menschen ihren Identitäten keinen großen finanziellen Wert beimessen. Identitätenhändler können ihren Rohstoff „digitale Identitäten“ zumeist kostengünstig durch geringe Anreize wie die Auslobung von kleinen Give-aways oder Preisen z.B. in Form von Preisausschreiben erlangen. Welche Vor- bzw. Nachteile dem Verbraucher durch die Preisgabe seiner digitalen Identität entstehen, dürften diesem aufgrund der komplexen Zusammenhänge nur unzureichend bekannt sein. Überlegungen, ob man die Verkettung von digitalen Identitäten überhaupt verhindern kann und welche Kosten der Schutz der persönlichen Daten verursacht, werden wahrscheinlich nur bei den wenigsten Verbrauchern in die Preisbildung für die Weitergabe der eigenen digitalen Identitäten einfließen.

2.3.5.3 Digitale Identitäten als Wirtschaftsgut

Digitale Identitäten können verkettet werden und auf dem Markt als ein neues qualitativ hochwertigeres Produkt angeboten und nachgefragt werden. Die Verkettung von digitalen Identitäten kann dabei grundsätzlich zwei Ziele verfolgen, die sich auch kombinieren lassen:

- Auf die Person zugeschnittenes Marketing:
  Um Produkte ohne große Streuverluste bei potenziellen Interessenten zu bewerben und diese auf eine geeignete Art anzusprechen, sollen möglichst viele Informationen der Person, hier in Form von verschiedenen digitalen Identitäten, miteinander verkettet analysiert werden, insbesondere in Hinblick auf Interessen, Kaufkraft und psychologische Eigenschaften zu ihrer geeigneten Ansprache und Gewinnung ihrer Aufmerksamkeit.

- Identifikation von Multiplikatoren:
  Verkettet man nicht nur Daten von einzelnen Personen, sondern analysiert auch, mit wem diese Personen in Beziehung stehen, lassen sich soziale Netzwerke ermitteln: Mit Kenntnis der Beziehungen in einem Freundes-, Verwandtschafts- oder Geschäftskreis können Personen mit besonders vielen Kontakten als Multiplikator ermittelt werden. Diese potenziellen Multiplikatoren können dann gezielt und aufwändig beworben werden in der Hoffnung, dass der Werbeinhalt über das überdurchschnittlich große soziale Netzwerk weitergegeben wird. Die Werbebotschaft wird hier in einem privaten Rahmen weitergegeben. Sie erreicht damit mehr Aufmerksamkeit und wird oft als vertrauenswürdiger oder authentischer empfunden als die Produktaussagen direkt von einer Firma. Dafür müssen aber Personen mit vielen oder einflussreichen Sozialbeziehungen identifiziert und von dem Produkt überzeugt werden.

Daneben unterscheidet man, ob die Sammlung und Verkettung von digitalen Identitäten originärer Geschäftszweck ist, dies die Grundlage für weiteres unternehmerisches Handeln darstellt oder solche Daten von anderen Unternehmen eingekauft werden:

- Verkettung als originärer Unternehmenszweck:
  Unternehmen wie Identitätenhändler verketten die digitalen Identitäten, um sie dann als eigenständiges neues Produkt zu vermarkten. Das Gut „digitale Identitäten“ wird in dem Wertschöpfungsprozess zu einem neuem Gut „verkettete digitale Identitäten“ mit höherem Nutzen transformiert.

- Verkettung als Grundlage für weiteres unternehmerisches Handeln:
  Solche Unternehmen verketten Identitäten nicht, um diese am Markt zu handeln, sondern um den Gewinn in der Kernkompetenz zu maximieren. Sie nutzen dabei das Wissen über die verketteten Identitäten, um ihre Produkte besser vermarkten zu können. Als Beispiel sei hier die Firma Google genannt, die über ihre verschiedenen Dienste wie Suchmaschine und E-Mail (Gmail) eine Vielzahl an Daten und Identitäten sammelt und diese wahrscheinlich für die optimale Vermarktung seiner Online-Werbung einsetzt.

- Hinzukaufen von verketteten digitalen Identitäten:
  Viele Unternehmen kaufen digitale Identitäten hinzu und verketten diese mit dem eigenen Datenbestand, um diesen anzureichern. In Unternehmenszusammenschlüssen wie Konzernen werden teilweise die Datenbestände der Tochterunternehmen zusammengeführt, um einen aussagekräftigeren Datenbestand zur Unterstützung der Marketing- und die Verkaufsaktivitäten zu generieren[119]. Rechtliche Einschränkungen im deutschen und europäischen Datenschutzrecht werden in diesen Fällen aufgrund der hierarchischen Konzernstruktur oder der verlockenden Wettbewerbsvorteile ignoriert[120].

[119] Vgl. 25. Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Textziffer 6.3.6 (Datenübermittlung zwischen Autohändlern und Automobilherstellern) sowie [Weichert 1996]. Außerdem siehe die Darlehensbedingungen der Volkswagenbank, Blatt 2 vom 05.07.2004.

[120] Siehe Schulzki-Haddouti, „Kundenkartei als Kapital“ im Handelsblatt Nr. 110 vom 12.06.2007; Kary, „Mitarbeiter- und Kundendaten: Fast alles ist möglich“ bei DiePresse.com vom 15.07.2007 sowie Artikel „Datenschutz in Gefahr: 'Dot-Coms' verscherbeln Kundendaten“ des Computer-Informations-Diensts vom 10.07.2000.

Verkaufsfördernde Aktivitäten können durch die Verkettung von Identitäten ebenso gesteuert werden wie die After-Sales-Aktivitäten des Unternehmens. Durch die Verkettung der digitalen Identitäten kann über die Verbraucher bzw. Kunden eine Reihe von zusätzlichen Erkenntnissen gewonnen werden, die dem Unternehmen helfen, die bestehenden Unternehmensressourcen möglichst gewinnbringend einzusetzen. Kunden können so nicht nur entsprechend ihrem Verhalten gegenüber dem Unternehmen, sondern aufgrund ihres gesamten Kaufverhaltens kategorisiert werden. Unter dem Begriff Scoring[121] wird das Bewerten von Verbrauchern zusammengefasst. Beschränkte sich das Scoring anfänglich auf die Kreditwürdigkeit, so wird das Scoring von Verbrauchern in vielen Wirtschaftsbereichen durchgeführt und beschreibt das Risiko und Potenzial von Kunden und potenziellen Kunden. Durch das Scoring werden Aktivitäten auf die Kunden gelenkt, die z.B. eine hohe Kaufkraft oder einen Multiplikatorenwirkung versprechen. Kunden, denen das Unternehmen durch das Scoring ein hohes Kaufpotenzial zuspricht, werden vielleicht schneller und mit mehr Serviceleistungen versorgt, als Kunden, die schlechte Umsätze erwarten lassen. Inbound-Callcenter können aufgrund der Rufnummernerkennung bestimmte Kundengruppen bevorzugt behandeln, während „schlechte“ Kunden oder Interessenten in die Warteschleife geschickt werden[122]. Unternehmer werden auch in dem Bereich Callcenter bestrebt sein, ihre Ausgaben am effektivsten und verkaufsförderndsten einzusetzen.

2.3.5.4 Vorteile durch Verkettung digitaler Identitäten für die Unternehmen

Für Marktforschung und Marketing wären „gläserne Konsumenten“ praktisch, um das komplexe Kaufverhalten der Verbraucher zu ergründen. Daher wird versucht, an Daten über das Verhalten der Konsumenten zu gelangen und dem gläsernen Verbraucher ein Stück näher zu kommen. Unternehmen versprechen sich von einem Mehr an persönlichen Daten einen Vorteil im Verteilungskampf um Marktanteile.

Die Verkettung von digitalen Identitäten kann für ein Unternehmen nur wirtschaftlich und damit interessant sein, wenn die positiven Effekte (Umsatz, Gewinn oder Image usw.) größer sind als die Kosten für die Beschaffung und Verkettung der digitalen Identitäten. Zusätzlich wird sich das Nutzen von digitalen Identitäten nur durchsetzen, wenn die gleichen Ergebnisse mit den herkömmlichen Instrumenten des Marketings aufwändiger zu erreichen sind. Besonders für Unternehmen, die gegenüber ihren Kunden Preisdifferenzierung betreiben möchten, dürften personenbezogene Konsumentendaten wie digitalen Identitäten von besonderem Interesse sein. Die Preisdifferenzierung beschreibt dabei den Zustand, dass Unternehmen gegenüber ihren Kunden versuchen, unterschiedliche Preise für gleiche Güter zu realisieren, ohne dass sich diese Preisunterschiede durch Kostenunterschiede begründen lassen. Es ist dabei das Ziel des Unternehmens, von jedem Kunden den Preis zu verlangen, den dieser maximal zu zahlen bereit ist. Das Unternehmen kann damit seinen Umsatz, im Gegensatz zu einem für alle Abnehmer einheitlichen Marktpreis, maximieren.

Ein Unternehmen, das langfristig am Markt erfolgreich agieren und bestehen möchte, sollte bei seinen unternehmerischen Aktivitäten nicht nur auf den temporären Vorteil schauen, sondern auch die Außenwirkungen des unternehmerischen Handelns berücksichtigen. Der Einsatz von Verkettung digitaler Identitäten als Instrument ist nicht unumstritten – das sollten Unternehmen berücksichtigen. Verbraucher- und Datenschützer warnen Verbraucher vor den Risiken der Preisgabe der eigenen digitalen Identitäten. Unternehmen, die in der Öffentlichkeit stehen, drohen Imageverluste, wenn zweifelhafte Geschäftspraktiken im Zusammenhang mit der Verwendung von digitalen Identitäten publik werden. Die Verbraucher könnten vermuten, das Unternehmen versuche sie auszuspionieren und zu übervorteilen.

Bei der Nutzung neuer Technologien gibt es neben den Vorteilen auch Einflussfaktoren, die die Einführung nachhaltig negativ beeinflussen können. Bei digitalen Identitäten ist zurzeit das größte Bedrohungsszenario der Identitätsdiebstahl. Solange die Haftungsfragen bei Identitätsdiebstählen im Zusammenhang mit digitalen Identitäten nicht eindeutig geklärt sind, werden Wirtschaftsunternehmen entweder nach selbst auferlegten ethischen Richtlinien entscheiden oder das monetäre Risiko

[121] Hierzu siehe den Abschnitt 3.3.4 dieser Arbeit sowie ausführlich das [ULD-Scoring-Gutachten 2006, S. 11 ff.].
[122] Von der Hagen, „Das ganze Leben in einer Zahl“ in der Süddeutschen Zeitung vom 15.07.2005.

nüchtern in die Geschäftskalkulationen einfließen lassen.[123] Bei der Kalkulation werden die Kosten für die Verhinderung von Identitätsdiebstählen dem Risiko, den Schaden des Identitätsdiebstahls tragen zu müssen, und der Höhe des Schadens gegenübergestellt. Neben den finanziellen Schadensszenarien wird sich die Wirtschaft auch Konzepte überlegen müssen, damit Verbraucher, die ihre digitalen Identitäten nicht den Wirtschaftsunternehmen zur Verfügung stellen möchten, geschützt werden und die Unternehmen in dieser Kundengruppe keinen Imageschaden erleiden. Ob sich Konzepte wie Robinsonlisten[124] übertragen lassen, wird sich noch zeigen müssen.

2.3.5.5 Unternehmensethik und Datenschutz

Unabhängig davon, ob ein Unternehmen nach dem Shareholder-Value-Konzept[125] oder dem Stakeholder-Ansatz[126] geführt wird, bedarf es weiterer Definition des Unternehmensziels und der Festlegung von Rahmenbedingungen. Anteilseigner und Aktionären fordern individuelle Unternehmensrichtlinien, denn Unternehmen stehen in der Öffentlichkeit, und ein Imageverlust wirkt sich direkt auf den Wert des Unternehmens aus. Unternehmen definieren in Ethikleitlinien ihre moralischen Wertevorstellungen und legen einen Verhaltenskodex fest, der beispielsweise regelt, wie mit Mitarbeitern, Kollegen, Kunden. Lieferanten oder der Umwelt umzugehen ist. Diese Ethikgrundsätze gelten dabei nicht nur für Vorgesetzte, sondern für alle Mitarbeiter und sollen als Unternehmenskultur gelebt werden und Motivation, Loyalität und damit die Produktivität steigern.

Unethisches Verhalten kostet Unternehmen zumeist viel Geld. Unternehmen, die sorglos mit der Umwelt oder „unfair“ mit den eigenen Kunden umgehen, erleiden bei Bekanntwerden schnell einen Imageschaden. Unternehmen, die Mobbing nicht ernst nehmen, müssen mit einer sinkenden Arbeitsleistung rechnen und können zu hohen Schadensersatzforderungen verurteilt werden. Zudem fallen auch die eigenen Mitarbeiter durch besonders unethisches Verhalten auf, denn Wirtschaftskriminalität wird zu einem großen Teil von den eigenen Mitarbeitern verübt.[127]

Der Umweltschutz ist sicherlich ein Thema, das die Ethikdebatte in Unternehmen vorangebracht hat und in den Ethiklinien seinen Platz gefunden hat. Der Stellenwert von personenbezogenen Daten nimmt aufgrund der weitreichenden Folgen neuer technischen Entwicklungen zu. Das Bekenntnis von Unternehmen zu Datenschutz und dem ethischen Umgang mit persönlichen Daten gehört damit nicht nur in die AGBs, sondern insbesondere auch in die Leitlinien für Unternehmensethik.

Ziel beim Festlegen von ethischen Grundsätzen von Unternehmen ist es nicht nur, das Gewissen zu beruhigen, sondern den Unternehmenswert zu steigern. Aktionäre und Investoren ziehen für ihre Entscheidungen neben Bilanzen und Umsatzzahlen auch die „Softskills“ eines Unternehmens zu Rate.

Ethisches Handeln heißt den Cashflow langfristig zu maximieren. Wer aus ethischen Gründen auf einen Teil seines kurzfristigen Umsatzes verzichtet, wird nach den Ansätzen der Wirtschafts- und Unternehmensethik langfristig aufgrund zufriedenerer Stakeholder profitieren. Ethik und Datenschutz werden durch geschickte Öffentlichkeitsarbeit für Unternehmen zum Wettbewerbsvorteil.

2.3.5.6 Die großen Unbekannten: Der Verbraucher und der Markt

Verkettung digitaler Identitäten als Marketingmethode wird sich der Frage stellen müssen, ob sie den gewünschten Erfolg erzielt und dadurch der Erfolg der Unternehmen steigen wird. Eine Antwort wird sich nicht rein theoretisch und kurzfristig ermitteln lassen, sondern ist nur empirisch über einen

123 [Roberto 2002, S. 26]; [Schmid 2006].

124 Der Ursprung der Robinsonliste liegt in der Briefwerbung. In der Robinsonliste können sich die Personen registrieren lassen, die keine unaufgeforderte Briefwerbung erhalten möchten.

125 Nach dem Shareholder-Value-Konzept ist das Management bei seinen Entscheidungen und Handlungen ausschließlich den Eigentümern des Unternehmens verpflichtet. Das einzige Ziel besteht darin, den Unternehmenswert zu steigern.

126 Bei dem Stakeholder-Ansatz ist das Management mehreren Interessengruppen (Mitarbeitern, Lieferanten, Kunden etc.) eines Unternehmens verpflichtet. Es ist die Aufgabe des Managements, die Ansprüche der Interessengruppen auf Relevanz zu prüfen.

127 Schaumann, „Business Ethik“ bei securitymanager.de (11/2006).

längeren Zeitraum belegbar. Die zentrale Frage dabei ist, wie flexibel der Verbraucher wirklich ist und ob er sich durch die ausgeklügelten Marketingmaßnahmen zum Produktwechsel animieren lässt.

Neue und interaktive Medien fördern augenscheinlich die Flexibilität der Verbraucher bei ihren Kaufentscheidungen.[128] Verbraucherorganisationen und Medien klären die Bürger über ihre Rechte als Verbraucher auf, und im Internet wird über spezielle Internetportale der Austausch von Preisinformationen und Produktmeinungen forciert.[129] Alle diese Entwicklungen sprechen für den mündigen und flexiblen Verbraucher, der auf kleine Marktveränderungen mit einem Produkt- oder Anbieterwechsel reagiert, um sich Vorteile am Markt zu sichern.

Jedoch werden in einigen Branchen von den Anbietern immer größere Prämien ausgelobt, um die Verbraucher zu einem Anbieterwechsel zu bewegen. Die Direktbanken sehen sich durch den Wettbewerb im Bankensektor dazu veranlasst, Neukunden bis zu 100 EUR an Prämien für eine Kontoeröffnung anzubieten. Es scheint so, dass es nicht auf die reinen Produkteigenschaften, wie z.B. die Verzinsung auf dem Konto ankommt, sondern bei der „Kaufentscheidung“ auch andere Kriterien wie z.B. die Prämie für Neukunden eine Rolle spielen. Aufgrund solcher Marktbesonderheiten ist es fraglich, ob es wirklich immer die Flexibilität der Verbraucher ist oder ob es nicht viel eher die ausgeklügelte Marketinginstrumente sind, die den Verbraucher in der Kaufentscheidung beeinflussen.

Der Erfolg eines Unternehmens am Markt wird neben den komplexen Kaufentscheidungen der Verbraucher auch durch das Verhalten der Mitbewerber beeinflusst. Das Verhalten der Marktteilnehmer (Verbraucher und Mitbewerber) ist zumeist wesentlich komplexer als die Annahmen in den verschiedenen Preis- und Absatzmodellen, wie die folgenden Beispiele zeigen. Unternehmen, die im Kampf um Marktanteile exzessiv zur Verkettung oder verketteten digitalen Identitäten greifen, könnten ihre Mitbewerber dazu veranlassen, den Kunden gegenüber herauszustellen, dass sie sehr verantwortungsvoll mit persönlichen Daten umgehen und sich an die Datenschutzgesetze halten. Dieses Vorgehen würde die gesamte Branche unter Zugzwang setzen. Auch wenn nur wenige Unternehmen die offene Vermarktung des Datenschutzes propagieren, werden in Zukunft die Verbraucher von jedem Unternehmen Aussagen zu deren Datenverarbeitung erwarten und diese Aussagen in die Kaufentscheidung einfließen lassen.

Es ist heute beobachtbar, dass sich Unternehmen, die eine langfristige Ausrichtung am Markt verfolgen, sich den gesellschaftlichen Werten stärker unterwerfen müssen als Unternehmen, die sich nur dem kurzfristigen Geschäftserfolg verschrieben haben.[130] Unternehmen, die ihren Erfolg in einem kurzen Agieren am Markt sehen, sind zwar in der Minderzahl,[131] werden aber mögliche Strafen für Datenschutzverstöße in ihr Nutzenkalkül einbeziehen und sich weniger um das Image bei den Verbrauchern sorgen.

Zusammenfassend lässt sich festhalten, dass erfolgreiches unternehmerisches Handeln mehr ist als das detaillierte Wissen über die Identitäten der potenziellen Kunden.

2.3.5.7 Ausblick: Digitale Identitäten, ein Markt mit Innovationen?

Das Nutzen verketteter digitalen Identitäten steht heute erst am Anfang seiner Möglichkeiten. Neben Marketing und Verkauf werden in Zukunft auch andere Lebensbereiche digitale Identitäten nutzen und die Vernetzung von persönlichen Daten vorantreiben. Diese gesellschaftlichen Entwicklungen werden nicht nur bei Anbietern von digitalen Identitäten neue Produktangebote generieren und neue Märkte erschließen, sondern es werden auch neue Geschäftsideen entstehen, die die Verbraucher vor der Verkettung von Identitäten schützen werden. Es wird sich zeigen, ob solche bereits theoretisch

[128] [Ahlert/Backhaus/Meffert 2001]; [Eckhardt et al. 2000, S. 5 ff].

[129] Einer Studie von Ipsos zufolge informieren sich 56 % aller Online-Käufer vor geplanten Neuanschaffungen in Internet-Meinungsforen. Siehe Puscher „Digitale Reputation – Wie vertrauenswürdig das Soziale Web ist“ in c't 10/2007, S. 142.

[130] [Hoppenstedt 2004, S. 33 f.].

[131] Bei einer Befragung von 1.210 österreichischen Unternehmen im Rahmen einer Studie der Initiative CSR Austria (Rücklaufquote: 20,1) gaben 75 % der antwortenden Unternehmen an, ein unternehmensspezifisches Wertesystem (Ethikleitbild) installiert zu haben – dieses kann als langfristige Unternehmensausrichtung interpretiert werden (siehe [Fischer-Hübner 2001, S. 11 f.]).

skizzierten oder in der Erprobungsphase stehenden Konzepte jetzt den Sprung in erfolgreiche Geschäftsmodelle vollziehen und sich somit wirtschaftlich unabhängig am Markt entfalten können.

Es gibt bereits erste Prototypen, die den Verbraucher vor der Beobachtung von Wirtschaftsunternehmen zu schützen versuchen, und weitere Konzepte, die Systeme für den anonymen und damit datenschutzfreundlichen Wirtschaftskreislauf entwickelt haben. Alle diese Dienste müssen jedoch noch den Wechsel zu einem wirtschaftlich eigenständigen am Markt agierenden Produkt schaffen. Dies hängt davon ab, inwieweit es den Betreibern gelingt, den Verbrauchern die Vorteile entsprechend transparent und den Mehrwert beim Schutz vor Weitergabe ihrer digitalen Identitäten plausibel zu machen. Neben den bereits bekannten Konzepten wird es neue Vermarktungskonzepte geben: Unternehmen könnten beispielsweise ihren Kunden kostenlos oder kostengünstig eine Software anbieten, mit denen sich diese vor den Risiken der Verkettung digitaler Identitäten schützen können. Denn was die Kunden für die Produkte der Mitbewerber oder in anderen Branchen ausgeben, könnte den Umsatz des Unternehmens schmälern. Jedes Unternehmen hat ein Interesse daran, die eigenen Kunden vor weiterer Verkettung zu schützen, die Mitbewerbern zum Vorteil gereichen könnte.

Ob sich neue Geschäftsideen und innovative Produkte am Markt durchsetzen werden, hängt von den Kosten und der Bedrohung durch Verkettung digitaler Identitäten für den Verbraucher ab. Nur wenn die Nachteile für Verbraucher durch die Verkettung digitaler Identitäten transparent und bezifferbar sind, werden solche Produkte am Markt bestehen können.

2.3.5.8 Die ökonomische Bedeutung digitaler Identitäten und ihrer Verkettung

Ökonomisch gesehen haben digitale Identitäten und deren Verkettung in den Wirtschaftskreislauf bereits Einzug gehalten, und ihre Bedeutung nimmt mehr und mehr zu. Zum einen finden digitale Identitäten und durch Verkettung und Anreicherung daraus entstehende Datenpools als Datenbasis für Marktforschung und Marketing Verwendung, zum anderen sind diese Informationen zu einem eigenständigen Produkt geworden, das als Wirtschaftsgut am Markt gehandelt wird.

Digitale Identitäten und deren Verkettung stehen erst am Anfang ihrer technischen Möglichkeiten, so dass auf diesem Markt aus technischer und soziologischer Sicht eine Reihe von innovativen Entwicklungen zu erwarten ist. Es wird dabei darauf zu achten sein, dass datenschutzrechtliche Belange beim Streben nach dem gläsernen Konsumenten nicht aus dem Auge verloren werden.

Mit welcher Geschwindigkeit und Intensität sich die Nutzung digitaler Identitäten im Marktgeschehen etablieren werden, wird zum größten Teil von dem erwarteten Nutzen abhängen. Wie hoch dieser Nutzen sein wird, bedarf jedoch noch empirischer Belege.

3 Status Quo hinsichtlich der Verkettung digitaler Identitäten

3.1 Einleitung

Die Verkettung digitaler Identitäten kann in unterschiedlichen sozialen Kontexten eine Rolle spielen:

Will etwa der Staat seinen Aufgaben nachkommen, so ist er auf Informationen über seine Bürger angewiesen. In diesem Zusammenhang stellen Register (z.B. das Melderegister), in denen bestimmte Sets von Daten über die Bürger gespeichert und bei Bedarf aktualisiert werden, ein wichtiges Instrument dar. Häufig finden im staatlichen Bereich auch Kennziffern, die dem jeweiligen Bürger zugeordnet werden, Verwendung. Es existiert also eine Vielzahl an staatlichen Datenbanken und Identifiern, die von unterschiedlichen hoheitlichen Stellen genutzt werden können. Es liegt auf der Hand, dass die vorhandenen Datenbestände – rein technisch gesehen – miteinander verkettbar sind und in vielen Fällen auch verkettet werden.

Auch im Verhältnis von Verbraucher und Unternehmen spielt die Verkettung von Daten eine immer größer werdende Rolle. Unternehmen horten alle Informationen über ihre Kunden, derer sie habhaft werden können, und erstellen mittels Techniken wie Data Warehousing und Data Mining immer exaktere und umfangreichere Kundenprofile. Hiervon versprechen sie sich zum einen Vorteile gegenüber Wettbewerbern (z.B. durch Strategien wie personalisierte Werbung oder Preisdiskriminierung), zum anderen eine Minimierung von Risiken (z.B. hinsichtlich eines möglichen Zahlungsausfalls potenzieller Kreditnehmer).

Schließlich spielt die Verkettung digitaler Identitäten auch im Bereich der Internet-Communities eine wichtige Rolle. Bei solchen Communities handelt es sich um Gemeinschaften von Menschen, die sich via Internet und mittels extra hierfür eingerichteter Plattformen begegnen und austauschen. Beispielhaft genannt seien an dieser Stelle nur MySpace, Xing oder Second Life[132]. Hier stellen Mitglieder oft freiwillig eine Vielzahl an Daten über ihre Person zur Verfügung und ermöglichen durch dieses Verhalten nicht zuletzt auch die Verkettung unterschiedlicher Datenbestände.

Nachfolgend werden für jeden dieser drei Bereiche (Bürger-Staat, Verbraucher-Unternehmen und Communities) exemplarisch bereits bestehende Verkettungen vorgestellt.

3.2 Verhältnis Bürger – Staat

3.2.1 Allgemeiner rechtlicher Abriss

3.2.1.1 Rechtsgrundlagen für eine Verkettung personenbezogener Daten

Wie bereits an anderer Stelle ausgeführt[133], gilt für jede Verarbeitung personenbezogener Daten und somit auch für deren Verkettung das Verbot mit Erlaubnisvorbehalt. Danach ist eine Verkettung personenbezogener Daten nur dann zulässig, wenn sie aufgrund einer Rechtsvorschrift oder einer Einwilligung des Betroffenen erfolgt. Im Verhältnis von Bürger und Staat wird eine solche Verkettung regelmäßig auf der Grundlage einer Rechtsvorschrift vorgenommen werden – eine Einwilligung wird hier dagegen kaum eine Rolle spielen[134].

[132] Die jeweilige Website ist abrufbar unter http://www.myspace.com/, http://www.xing.com/ und http://secondlife.com/ (letzte Zugriffe jeweils im Oktober 2007).

[133] Vgl. unter 2.3.3.1.4 (Juristische Grundlagen: Rechtliche Einordnung von Verkettung/Verkettbarkeit).

[134] Dies hängt schon damit zusammen, dass Voraussetzung für eine wirksame Einwilligung eine freie Entscheidung des Betroffenen ist. Zur Erfüllung seiner Aufgaben benötigt der Staat aber eine Vielzahl an Daten, deren Verwendung er nicht von der freiwilligen Zustimmung des Bürgers abhängig machen kann.

Insoweit sind die vielen unterschiedlichen bereichsspezifischen Vorschriften zu beachten, die jeweils regeln, unter welchen Voraussetzungen eine Verwendung personenbezogener Daten in bestimmten Kontexten zulässig ist. Das Bundesdatenschutzgesetz bzw. die Landesdatenschutzgesetze sind als sog. Auffanggesetze hingegen nur dann anwendbar, wenn im konkreten Einzelfall keine dieser bereichsspezifischen Regelungen einschlägig ist[135]. Dabei sind die entsprechenden Bestimmungen des Bundesdatenschutzgesetzes[136] anwendbar, wenn personenbezogene Daten durch öffentliche Stellen des Bundes erhoben, verarbeitet oder genutzt werden, wohingegen die Landesdatenschutzgesetze bei einer Datenverarbeitung durch öffentliche Stellen des jeweiligen Landes einschlägig sind.

Aufgrund der Vielzahl bereichsspezifischer Gesetze ist es an dieser Stelle nicht möglich, vorab einen kurzen Überblick über eventuell einschlägige Rechtsnormen für eine Verkettung von Daten im staatlichen Bereich zu geben. Stattdessen ist bei jedem der Beispiele, die in diesem Kapitel vorgestellt werden, einzeln darzustellen, auf welcher rechtlichen Grundlage die jeweilige Datenverarbeitung stattfindet.

Bevor die einzelnen Beispiele vorgestellt werden, wird auf zwei rechtliche Themenkomplexe eingegangen, die gerade hinsichtlich der Vornahme von Verkettungen im Verhältnis von Staat und Bürger eine wichtige Rolle spielen: die verfassungsrechtliche Unzulässigkeit der Verwendung eines einheitlichen staatlichen Personenkennzeichens sowie gesetzliche Identifizierungspflichten des Bürgers gegenüber staatlichen Stellen.

3.2.1.2 Verwendung von Personenkennzeichen

Personenkennzeichen (PKZ) bestehen aus Kombinationen alphanumerischer Zeichen und sind einer bestimmten Person zugeordnet[137]. Anhand eines PKZ lassen sich Daten einfach zusammenführen – ein solches Kennzeichen erleichtert also eine Verkettung personenbezogener Daten.

In Deutschland fand schon Ende der 60er Jahre eine Diskussion über Personenkennzeichen statt[138]. Im Zuge dieser Debatte wurde sehr schnell klar, dass insbesondere solche Kennzeichen, die einzigartig sind, universell eingesetzt werden und lebenslang gültig sind, zur Erstellung umfassender Persönlichkeitsprofile verwendet werden können[139].

Das Bundesverfassungsgericht erklärte deshalb bereits in seiner Mikrozensusentscheidung[140] aus dem Jahre 1969 die Erstellung von Persönlichkeitsprofilen, ohne dass der Betroffene deren Richtigkeit und Verwendung zureichend kontrollieren kann, für unzulässig. Diese Einschätzung bekräftigte das Gericht noch einmal in dem schon erwähnten Volkszählungsurteil von 1983. Auch dieser Entscheidung liegt die Überlegung zugrunde, dass ein (universelles) Personenkennzeichen eine einfache Verkettung verschiedener Daten und damit eine umfassende Registrierung und Katalogisierung der Persönlichkeit sowie eine Erstellung umfangreicher Persönlichkeitsprofile der Bürger ermöglichen würde[141].

Die soeben skizzierte verfassungsgerichtliche Rechtsprechung, wonach die Verwendung eines einheitlichen Personenkennzeichens unzulässig ist, war bisher der Garant dafür, dass in Deutschland lediglich sektorspezifische Personenkennzeichen genutzt werden[142]. Mittlerweile gibt es aber Stimmen in der rechtswissenschaftlichen Literatur, denen zufolge das Verbot eines einheitlichen PKZ aufgrund der Entwicklung der Informationstechnik nicht mehr zeitgemäß ist, da Daten auch ohne eine solche

[135] Vgl. §§ 1 Abs. 3 S. 1 BDSG, 3 Abs. 3 LDSG SH.
[136] Vgl. insbes. §§ 12 ff. BDSG.
[137] Den Begriff des Personenkennzeichens erläutert [Bizer 2004].
[138] Auslöser hierfür waren Pläne der damaligen Bundesregierung, ein Verbundsystem für alle staatlich gesammelten Daten einzuführen und in diesem Zusammenhang jedem Bürger ein lebenslang gültiges PKZ zuzuweisen.
[139] Vgl. [Weichert 2002].
[140] Beschluss vom 16.07.1969: BVerfGE 27, 1 = NJW 1969, 1707.
[141] BVerfGE 65, 1 (53).
[142] Allerdings sei an dieser Stelle darauf hingewiesen, dass etwa in den skandinavischen Staaten diese Bedenken nicht geteilt werden, weshalb dort auch seit geraumer Zeit einheitliche Personenkennzeichen verwendet werden.

Nummer verkettet werden können[143]. Dem ist aber entgegenzuhalten, dass eine Verkettung durch ein universelles PKZ noch zusätzlich erleichtert und effektiviert wird, weshalb am Verbot eines solchen Personenkennzeichens festzuhalten ist[144]. Diese Problematik gewinnt gegenwärtig angesichts der Einführung der neuen staatlichen Identifikationsnummer, die in der zweiten Jahreshälfte 2007 ausgegeben werden soll, wieder einmal an Brisanz: Es ist nämlich nicht auszuschließen, dass diese Nummer im Zuge der bevorstehenden Zentralisierung des Meldewesens zu einem einheitlichen Personenkennzeichen ausgebaut werden könnte.

3.2.1.3 Identifizierungspflichten gegenüber staatlichen Stellen

3.2.1.3.1 Überblick

Wie bereits erwähnt, sind die Datenschutzgesetze nur anwendbar, wenn Daten erhoben, verarbeitet oder genutzt werden, die einen Personenbezug aufweisen, d.h. eine bestimmte oder zumindest bestimmbare Person betreffen. Grundsätzlich steht einer und einem jeden das Recht zu, anonym aufzutreten und hierdurch einen Personenbezug zu verhindern. Diese Möglichkeit scheidet allerdings dann aus, wenn die betroffene Person eine gesetzliche Pflicht zum Nachweis ihrer Identität trifft.

Für den Bürger bestehen gegenüber staatlichen Stellen vielerlei Identifizierungspflichten. Von besonderer Relevanz sind diese im Bereich der Strafverfolgung und der Gefahrenabwehr[145]. Weitere wichtige Verpflichtungen zur Angabe der eigenen Identität finden sich z.B. im Ordnungswidrigkeiten- und im Ausländerrecht[146]. Auch das jeweils einschlägige Prozessrecht sieht Identifizierungspflichten vor[147].

Der Pflicht des Betroffenen korrespondiert dabei jeweils eine gesetzliche Befugnis der zuständigen Stelle zur Feststellung der Identität.

Nachfolgend werden exemplarisch wichtige Identifizierungspflichten von Bürgern gegenüber der Polizei sowie das Erfordernis der Offenlegung der eigenen Identität als Voraussetzung für die Inanspruchnahme staatlicher Dienstleistungen näher beleuchtet.

3.2.1.3.2 Identifizierungspflichten gegenüber der Polizei

Es gibt kaum ein polizeiliches Handeln, das nicht von einer Identitätsfeststellung begleitet wird, weshalb es sich bei der Feststellung der Identität um eine der wichtigsten polizeilichen Standardmaßnahmen handelt.

Im Bereich der Gefahrenabwehr kann die Polizei nach den jeweils einschlägigen Landesgesetzen unter bestimmten Voraussetzungen die Identität einer Person feststellen[148]. Eine solche Befugnis wird ihr insbesondere zur Abwehr einer konkreten Gefahr und gegenüber Personen, die sich an sog. gefährlichen Orten aufhalten, eingeräumt.

Im Strafverfolgungsbereich dürfen Polizei und Staatsanwaltschaft alle Maßnahmen treffen, die zur Ermittlung der Identität einer Person, die einer Straftat verdächtig ist, erforderlich sind[149]:

---

143 So etwa Podlech in [AK-GG 2001, Art. 2 Abs. 1 Rn. 79 und Fn. 115].

144 Ausführlich hierzu [Weichert 2002, S. 173].

145 Vgl. insbesondere § 181 LVwG SH und § 163b, c StPO.

146 §§ 163 b, c StPO analog i.V.m. 46 I OWiG, 49 AufenthG.

147 So regelt etwa § 68 StPO, dass zu Beginn jeder Zeugenvernehmung die Feststellung der Personalien erfolgt. Dabei ist der Zeuge auch dann dazu verpflichtet, die entsprechenden Angaben zu machen, wenn er von einem Zeugnisverweigerungsrecht Gebrauch macht.

148 Vgl. etwa § 181 LVwG SH.

149 § 163b Abs. 1 S. 1 1. HS StPO. Darüber hinaus kann gem. § 163b Abs. 2 StPO auch die Identität einer Person festgestellt werden, die einer Straftat nicht verdächtig ist, wenn und soweit dies zur Aufklärung der jeweiligen Tat geboten ist. Hier gehen die Befugnisse der Polizei allerdings nicht so weit wie gegenüber einer Person, die einer Straftat verdächtig ist.

Zu diesen Maßnahmen zählen das Anhalten des Verdächtigen, die Befragung nach seinen Personalien und die Aufforderung zur Aushändigung der von ihm mitgeführten Ausweispapiere zwecks Prüfung derselben. Kann die Identität sonst nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden, darf die verdächtige Person außerdem festgehalten und durchsucht werden. Gleiches gilt für die von dem Verdächtigen mitgeführten Sachen. Schließlich darf eine verdächtige Person zur Dienststelle verbracht und es dürfen erkennungsdienstliche Maßnahmen an ihr vorgenommen werden. Dies setzt ebenfalls voraus, dass die Identität sonst nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann.

Die obigen Ausführungen verdeutlichen, dass zur Feststellung der Identität unterschiedliche Maßnahmen zum Einsatz kommen können. Diese reichen von der bloßen Befragung hinsichtlich der Personalien bis zu erkennungsdienstlichen Maßnahmen – sofern die Identität anders nicht ermittelt werden kann, dürfen also auch Lichtbilder und Fingerabdrücke eines Beschuldigten aufgenommen und Messungen und ähnliche Maßnahmen an ihm vorgenommen werden[150]. Dies ist auch dann zulässig, wenn der Betroffene hiermit nicht einverstanden ist.

3.2.1.3.3 Anonyme Inanspruchnahme staatlicher Dienstleistungen

Auch wenn ein Bürger staatliche Dienstleistungen in Anspruch nehmen möchte, muss er regelmäßig seine Identität offenlegen und kann somit gegenüber den jeweils zuständigen Stellen nur ausnahmsweise anonym auftreten. Im Bereich des E-Government[151] bietet sich dem Bürger die Möglichkeit eines solchen anonymen Auftretens etwa dann, wenn er lediglich Informationen wie Adresse oder Öffnungszeiten einer Behörde via Internet einholen möchte.

Generell verbleibt es aber dabei, dass ein Bürger auch im Zusammenhang mit der Inanspruchnahme staatlicher Dienstleistungen zumeist nicht anonym auftreten kann. So setzt etwa der Erlass eines (begünstigenden) Verwaltungsaktes die eindeutige Angabe des jeweiligen Adressaten voraus. Zu den Anforderungen an die Bestimmtheit eines Verwaltungsaktes gehört es nämlich, dass die Identität des Adressaten zweifelsfrei bestimmt und Verwechslungen ausgeschlossen werden können[152]. Außerdem wird seitens der Verwaltung eine Vielzahl von Dienstleistungen erbracht, die zwar keinen Verwaltungsakt darstellen, aber die Vorlage des Personalausweises oder Reisepasses sowie die persönliche Vorsprache des Bürgers erfordern[153].

Auch der Bereich des E-Government bildet insoweit keine Ausnahme. So kommt [Gundermann 2003] zu dem Ergebnis, dass nur wenige E-Government-Angebote anonym oder pseudonym genutzt werden können. Sofern ein Schriftformerfordernis greift, das durch eine qualifizierte elektronische Signatur ersetzt werden kann, werden der Möglichkeit eines pseudonymen Auftretens zusätzlich durch verschiedene – insoweit – restriktive Rechtsvorschriften Grenzen gesetzt[154].

3.2.1.3.4 Nachweis der Identität mit Hilfe von Ausweisdokumenten

Wie bereits ausgeführt, wird es etwa in manchen Fällen im Bereich der Strafverfolgung erforderlich sein, erkennungsdienstliche Maßnahmen zu ergreifen. Vielfach wird sich die Identität einer Person jedoch schon mittels mitgeführter Ausweisdokumente feststellen lassen. Hierzu wird in erster Linie der Personalausweis verwendet. So dient denn auch die Verpflichtung aller Deutschen über 16 Jahre, einen solchen Personalausweis zu besitzen, primär dazu, ihn auf Verlangen einer zur Prüfung der Personalien ermächtigten Behörde vorzulegen[155].

---

150 § 163b Abs. 1 S. 3 i.V.m. § 81b 2. Var. StPO.

151 Einzelheiten hierzu im Abschnitt 3.2.5.

152 Vgl. [Gundermann 2003].

153 So zählt [Thiel 2006] allein für den Bereich des Meldewesens zehn verschiedene Dienstleistungen der Meldebehörden wie die Anmeldung bei der Meldebehörde oder die Ausstellung von Führungszeugnissen auf, für die dies gilt.

154 Vgl. §§ 3a Abs. 2 S. 3 VwVfG, 36 a Abs. 2 S. 3 SGB I, 87 a Abs. 3 S. 3 AO.

155 Insoweit sei noch angemerkt, dass in Deutschland keine Pflicht dazu besteht, den Personalausweis jederzeit mitzuführen – verpflichtet ist man lediglich dazu, den Ausweis auf Verlangen einer zur Identitätsfeststellung befugten Stelle vorzulegen.

Auch Ausländer sind in Deutschland zum Besitz eines gültigen Ausweisdokuments verpflichtet: Sie dürfen nämlich grundsätzlich nur dann ins Inland einreisen und sich dort aufhalten, wenn sie einen anerkannten und gültigen Pass besitzen[156]. Dieser ist den zuständigen Behörden auf Verlangen vorzulegen, auszuhändigen und vorübergehend zu überlassen[157].

Im Übrigen besteht ein wesentlicher Zweck des Meldewesens darin, die Identität von Personen feststellen und nachweisen zu können. So bestimmen das Melderechtsrahmengesetz und die verschiedenen Landesmeldegesetze, dass die Meldebehörden die in ihrem Zuständigkeitsbereich wohnhaften Personen zu registrieren haben, um deren Identität und Wohnungen feststellen und nachweisen zu können[158].

3.2.1.3.5 Verweigerung von Angaben zur Identitätsfeststellung

Wer von einer zuständigen Stelle dazu aufgefordert wird, Angaben zu identifizierenden Merkmalen wie Name, Geburtsdaten oder Adresse zu machen, hat dieser Verpflichtung nachzukommen. Verweigert er die entsprechenden Angaben – oder macht er unrichtige Angaben –, so handelt er ordnungswidrig. Diese Ordnungswidrigkeit kann mit einer Geldbuße geahndet werden[159].

Schon die bloße Verweigerung von Angaben zur Identität gegenüber einer zuständigen staatlichen Stelle führt also zu Sanktionen für den Bürger. Macht dieser unrichtige Angaben, kann dies in machen Fällen sogar strafrechtliche Konsequenzen nach sich ziehen[160].

3.2.1.4 Fazit

Im Verhältnis von Bürger und Staat kommen als Rechtsgrundlage für eine Verkettung personenbezogener Daten regelmäßig bereichsspezifische Regelungen in Betracht. Diese bereichsspezifischen Vorschriften gehen den subsidiären Regelungen des Bundesdatenschutzgesetzes bzw. der Landesdatenschutzgesetze vor.

Die Verwendung eines einheitlichen, bereichsübergreifenden staatlichen Personenkennzeichens ist nach der Rechtsprechung des Bundesverfassungsgerichtes unzulässig. Ein anonymes oder pseudonymes Auftreten des Bürgers gegenüber staatlichen Stellen ist dann nicht möglich, wenn er gesetzlich zur Offenlegung seiner Identität verpflichtet ist.

3.2.2 Staatliche Register

3.2.2.1 Einleitung

Im hoheitlichen Bereich stellen Register ein wichtiges Instrument zur Verkettung verschiedener personenbezogener Daten dar. Begrifflich handelt es sich bei Registern um systematische Sammlungen von Informationen über eine Gruppe von Objekten[161]. In Deutschland existiert eine Vielzahl hoheitlicher Register: So gibt es etwa das Melderegister, das Personalausweisregister, das Passregister, die Personenstandsbücher[162], die Grundbücher, die Führerscheinkartei, das Bundeszentralregister, das Verkehrszentralregister, das zentrale Fahrzeugregister, das Handelsregister, das

[156] § 3 Abs. 1 AufenthG.
[157] § 48 Abs. 1 AufenthG.
[158] §§ 1 Abs. 1 S. 1 MRRG, 2 Abs. 1 S. 1 LMG SH. Einzelheiten hierzu finden sich im Abschnitt 3.2.2 zu staatlichen Registern in dieser Arbeit.
[159] § 111 OWiG. Gem. Abs. 3 dieser Vorschrift kann die Geldbuße bis zu 1.000 EUR betragen.
[160] Hierzu siehe [Krasemann 2006a, S. 213 f.].
[161] Bei hoheitlichen Registern ist zwischen öffentlichen und beschränkt-öffentlichen Registern zu unterscheiden. Öffentliche Register sind solche mit unbeschränktem Zugang, wohingegen der Zugang zu beschränkt öffentlichen Registern nur unter bestimmten Bedingungen gewährt wird. Des Weiteren lassen sich zentral und dezentral geführte Register unterscheiden, wobei dieser Unterschied aufgrund der heutigen – technischen – Vernetzungsmöglichkeiten mehr und mehr an Bedeutung verliert.

Gewerbezentralregister, das Vereinsregister und das Ausländerzentralregister, um nur einige wichtige Register zu nennen.

Nachfolgend wird am Beispiel des Melderegisters demonstriert, welche Verkettungen von Daten hoheitliche Register ermöglichen. Danach wird kurz auf den künftigen registergestützten Zensus eingegangen und dargestellt, welche Daten aus welchen Registern in diesem Zusammenhang miteinander verkettet werden sollen.

3.2.2.2 Melderegister

3.2.2.2.1 Allgemeines

Das moderne Meldewesen soll primär zwei Funktionen erfüllen: Zum einen dient es der Feststellung der Identität und der Wohnung der Einwohner (Identifikationsfunktion), zum anderen der Erteilung von Auskünften hierüber an öffentliche und private Stellen (Informationsfunktion). Gegenwärtig ist das Melderecht noch im Melderechtsrahmengesetz (MRRG) und den Meldegesetzen der Länder geregelt. Allerdings haben sich Bund und Länder im Zuge der Föderalismusreform 2006 darauf verständigt, dass der Bund nunmehr die ausschließliche Gesetzgebungskompetenz für das Meldewesen hat[163]. Diese wird er in der näheren Zukunft durch die Verabschiedung eines Bundesmeldegesetzes ausfüllen. Die Verwaltungskompetenz, also die Zuständigkeit für die Ausführung des/der Meldegesetze(s), wird hiervon allerdings nicht berührt: Sie wird auch zukünftig bei den Ländern liegen und von den kommunalen Meldebehörden wahrgenommen werden[164]. Deren Aufgabe besteht darin, die Einwohner der jeweiligen Kommune zu registrieren, um ihre Identität und Wohnung feststellen und nachweisen zu können, Melderegisterauskünfte zu erteilen sowie bei der Durchführung von Aufgaben anderer Behörden oder sonstiger öffentlicher Stellen mitzuwirken und Daten zu übermitteln[165].

Die bei den kommunalen Meldebehörden geführten Melderegister sollen die Erfüllung dieser Aufgaben ermöglichen. Sie enthalten Daten, die bei den Betroffenen erhoben, von Behörden oder sonstigen öffentlichen Stellen übermittelt oder sonst amtlich bekannt werden[166]. Die Vollständigkeit und Richtigkeit der Melderegister wird sichergestellt durch ihre Fortschreibung von Amts wegen, durch Hinweise öffentlicher Stellen, die Daten aus den Registern erhalten haben und durch die allgemeine Meldepflicht[167].

3.2.2.2.2 Verkettung von Daten in den kommunalen Melderegistern

In den Melderegistern sind die folgenden Daten einschließlich der zum Nachweis ihrer Richtigkeit erforderlichen Hinweise zu speichern (siehe Tabelle 6):

[162] Während einer Übergangszeit vom 01.01.2009 bis zum 31.12.2013 werden die bisherigen Personenstandsbücher in Papierform von elektronischen Personenstandsregistern abgelöst. Die Rechtsgrundlage für diese Umstellung wurde durch das Personenstandsrechtsreformgesetz 2006 geschaffen, das am 23.02.2007 im Bundesgesetzblatt verkündet worden ist und dessen Regelungen im Wesentlichen am 01.01.2009 in Kraft treten werden.

[163] So jetzt Art. 73 Abs. 1 Nr. 3 GG.

[164] Vgl. Art. 83 f. GG.

[165] § 1 Abs. 1 S. 1 und 2 MRRG.

[166] § 1 Abs. 1 S. 4 MRRG.

[167] Vgl. §§ 4a (Fortschreibung von Amts wegen und Hinweise öffentlicher Stellen) und 11 (allgemeine Meldepflicht) MRRG.

Melderegisterdaten		
Familiennamen	frühere Namen	Vornamen
Doktorgrad	Ordensnamen/Künstlernamen	Tag und Ort der Geburt
Geschlecht	gesetzlicher Vertreter	Staatsangehörigkeiten
rechtliche Zugehörigkeit zu einer Religionsgesellschaft	gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung	bei Zuzug aus dem Ausland ggf. auch die letzte Anschrift im Inland
Tag des Ein- und Auszugs	Familienstand	Ehegatte oder Lebenspartner
minderjährige Kinder	Ausstellungsbehörde, Ausstellungsdatum, Gültigkeitsdauer und Seriennummer des Personalausweises/Passes	
Übermittlungssperren	Sterbetag und -ort	weitere Daten (siehe sogleich)

Tabelle 6: Im Melderegister gespeicherte Daten (1)

Darüber hinaus werden in den Melderegistern auch Daten zur Realisierung folgender Zwecke gespeichert (siehe Tabelle 7):

Melderegisterdaten (2)		
Daten für die Vorbereitung von Wahlen zum Deutschen Bundestag und zum Europäischen Parlament	Daten für die Ausstellung von Lohnsteuerkarten	Daten für die Ausstellung von Pässen und Personalausweisen
Daten für staatsangehörigkeitsrechtliche Verfahre	Daten für Zwecke der Suchdienste (Bundesvertriebenengesetz)	Daten für waffenrechtliche Verfahren
Daten für Zwecke der eindeutigen Identifizierung der Einwohner in Besteuerungsverfahren (steuerliche ID-Nummer)		Daten für sprengstoffrechtliche Verfahren

Tabelle 7: Im Melderegister gespeicherte Daten (2)

Schließlich kann durch Landesgesetz bestimmt werden, dass für die Erfüllung von Aufgaben der Länder weitere Daten gespeichert werden.

3.2.2.2.3 Anderweitige Verkettungen durch eine Übermittlung von Daten

Die obige Auflistung macht deutlich, dass bereits in den einzelnen Melderegistern selbst vielerlei personenbezogene Daten miteinander verkettet werden. Darüber hinaus geben die Meldebehörden in den folgenden Konstellationen Daten an andere öffentliche oder private Stellen weiter und ermöglichen somit eine Verkettung mit anderen Datenbeständen:

- Datenübermittlungen zwischen den Meldebehörden,
- Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen,
- Datenübermittlungen an öffentlich-rechtliche Religionsgemeinschaften,
- einfache Melderegisterauskunft,
- erweiterte Melderegisterauskunft.

Auf die entsprechenden Einzelheiten kann an dieser Stelle nicht näher eingegangen werden.

3.2.2.2.4 Folgen der Verkettung(en) für den Betroffenen

Allein anhand obiger Ausführungen dürfte bereits deutlich geworden sein, dass die heutigen Melderegister in vielerlei Hinsicht als Informationsfundus für öffentliche und private Stellen dienen und faktisch umfassende Verkettungen von Daten ermöglichen. Dies resultiert nicht zuletzt daraus, dass in ihnen mittlerweile auch eine Vielzahl von Angaben gespeichert wird, die nicht für die ursprünglichen Aufgaben des Meldewesens (Identifikation und Wohnung sowie Information hierüber) benötigt werden. Insoweit denke man nur an die steuerliche Identifikationsnummer oder Angaben über waffenrechtliche oder sprengstoffrechtliche Erlaubnisse. Wie bei jeder Verkettung und Speicherung einer großen Menge von Informationen besteht hier aus Sicht des Betroffenen das Risiko einer missbräuchlichen Verwendung und Weitergabe dieser Daten mit u.U. gravierenden Auswirkungen.

3.2.2.2.5 Betroffenenrechte und Transparenz der Verkettung(en)

Im geltenden Melderecht finden sich verschiedene Vorschriften, die die aus der Speicherung und Übermittlung vieler unterschiedlicher Daten resultierenden (Verkettungs-)Risiken beherrschbar machen sollen. So dürfen die Meldebehörden die soeben erwähnten Daten, die nicht für die ursprünglichen Aufgaben des Meldewesens benötigt werden, nur im Rahmen der in den jeweiligen Vorschriften genannten Zwecke verarbeiten oder nutzen. Außerdem werden dem Betroffenen gegenüber der jeweiligen Meldebehörde die folgenden Rechte eingeräumt[168]:

- Recht auf Auskunft;
- Recht auf Berichtigung und Ergänzung;
- Recht auf Löschung;
- Recht auf Unterrichtung über die Erteilung einer erweiterten Melderegisterauskunft;
- Recht auf Speicherung verschiedener Übermittlungssperren.

3.2.2.2.6 Zentralisierung des Meldewesens

Wie bereits erwähnt, hat der Bund seit der Föderalismusreform 2006 die ausschließliche Gesetzgebungskompetenz für das Meldewesen, die er in näherer Zukunft durch den Erlass eines Bundesmeldegesetzes auch ausüben wird. In diesem Zusammenhang plant die gegenwärtige Bundesregierung die Errichtung eines zentralen Melderegisters[169]. In technischer Hinsicht würde ein solches zentrales Register eine umfassende Registrierung aller Bürger mit überregionalem und ressortübergreifendem Zugriff ermöglichen. Sofern es tatsächlich zur Errichtung eines zentralen Registers kommen wird, so wird voraussichtlich auch die sog. steuerliche Identifikationsnummer in diesem gespeichert werden. Es ist nicht auszuschließen, dass diese Nummer nicht nur im Bereich des Steuerwesens, sondern sukzessive auch in anderen staatlichen Sektoren zum Einsatz kommen wird. Insoweit wird dann aber die bereits vorgestellte Rechtsprechung des Bundesverfassungsgerichts zur Unzulässigkeit eines einheitlichen Personenkennzeichens zu beachten sein.

3.2.2.2.7 Registergestützter Zensus

Bei einem Zensus (= Volkszählung) handelt es sich um eine Erhebung statistischer Bevölkerungsdaten, mittels derer insbesondere ermittelt wird, wie viele Menschen in einem Land bzw. in einer Stadt leben und wie sie wohnen und arbeiten. Von Bedeutung sind die hierbei ermittelten Daten etwa für die konkrete Ausgestaltung des Länder- bzw. des kommunalen Finanzausgleichs oder die Einteilung der Bundestagswahlkreise. Da die statistische Datenbasis mit zunehmendem zeitlichen Abstand zur jeweils letzten Volkszählung immer ungenauer wird, werden in den meisten Staaten in regelmäßigen Abständen Volkszählungen durchgeführt. In Deutschland war dies zuletzt 1987 (Bundesrepublik

[168] § 7 MRRG.

[169] Siehe die Meldung „Bericht: Bundesregierung plant zentrales Melderegister“ bei heise online, abrufbar unter http://www.heise.de/newsticker/meldung/83859/ (letzter Zugriff im Oktober 2007).

Deutschland) bzw. 1981 (Deutsche Demokratische Republik) der Fall – beide Volkszählungen liegen also schon (mehr als) zwei Jahrzehnte zurück.

Die Europäische Union plant für 2010/11 die Durchführung eines verbindlichen gemeinschaftsweiten Zensus. Eine entsprechende Rechtsverordnung werden der Rat und das Europäische Parlament voraussichtlich noch im Jahr 2007 erlassen.

Das Bundeskabinett hat im August 2006 beschlossen, dass dieser Zensus in Deutschland nicht als traditionelle Volkszählung, d.h. mittels einer Befragung der Bevölkerung, sondern als registergestützter Zensus durchgeführt werden soll[170].

Für diesen Zensus sollen Auswertungen der Melderegister, der Register der Bundesagentur für Arbeit sowie der Dateien zum Personalbestand der Öffentlichen Hand mit einer postalischen Gebäude- und Wohnungszählung sowie ergänzenden Stichprobenerhebungen verkettet werden[171]. Erste Vorarbeiten in rechtlicher Hinsicht sind bereits geleistet worden: Das Bundeskabinett hat Ende März 2007 den Entwurf eines Gesetzes zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2011 (Zensusvorbereitungsgesetz 2011 – ZensVorbG 2011) verabschiedet[172].

3.2.2.2.8 Fazit

An dieser Stelle soll nicht näher auf den geplanten registergestützten Zensus eingegangen werden. Entscheidend für den hier in Rede stehenden Kontext ist, dass die geplante Verkettung verschiedener Register und weiterer Daten – einmal mehr – deutlich macht, dass es kein gravierendes technisches Problem darstellt, Daten aus verschiedenen Registern miteinander zu verketten. Benötigt werden insoweit lediglich gemeinsame Datenformate und Schnittstellen[173].

Die kommunalen Melderegister stellen eine Vielzahl von Daten über jeden Bürger zur Verfügung, die nach einer Übermittlung an andere Stellen von diesen mit ihren Datenbeständen verkettet werden können. Das für die Zukunft angekündigte zentrale Melderegister wird eine Verkettung dieser Daten noch leichter machen.

3.2.2.2.9 Annex: Europäische Melderegisterauskunft RISER

Wie E-Government-Dienste im Bereich des Meldewesens datenschutzgerecht – auch im Hinblick auf mögliche Verkettungen – ausgestaltet werden können, zeigt die europäische Melderegisterauskunft RISER (Registry Information Service on European Residents)[174], die im Rahmen eines vom eTEN-Programm der Europäischen Kommission geförderten Projekts entwickelt worden ist.

RISER bietet seinen Kunden einen einheitlichen Zugang zu einer sehr heterogenen und unübersichtlichen Landschaft von Melderegistern in Europa. Über das Service-Portal für Meldeanfragen werden Datei- oder Einzelanfragen via Internet an die zuständige Meldebehörde weitergeleitet und von dort beantwortet. RISER übernimmt dabei die Funktion eines Zustellers.

Ein wichtiger Aspekt in diesem Zusammenhang ist die datenschutzgerechte Ausgestaltung des Dienstes. Insoweit wurden bei der Einführung von RISER insbesondere die folgenden Fragestellungen berücksichtigt, an denen sich auch alle Weiterentwicklungen des Dienstes zu orientieren haben:

---

[170] Siehe die Meldung „Bundesregierung beschließt registergestützte Volkszählung“ bei heise online, abrufbar unter http://www.heise.de/newsticker/meldung/77447/ (letzter Zugriff im Oktober 2007).

[171] Nähere Informationen der Statistischen Ämter des Bundes und der Länder zum registergestützten Zensus können unter http://www.zensus2011.de/ abgerufen werden (letzter Zugriff im Oktober 2007).

[172] Hierzu vergleiche die Meldung „Bundeskabinett verabschiedet Zensusvorbereitungsgesetz“ bei heise online, abrufbar unter http://www.heise.de/newsticker/meldung/87523/ (letzter Zugriff im Oktober 2007).

[173] Im Bereich des Meldewesens gibt es mit OSCI-XMeld bereits die Spezifikation eines bundeseinheitlichen Datenaustauschformates für die Übermittlung von Meldedaten.

[174] http://www.riser.eu.com/ (letzter Zugriff im Oktober 2007).

- Welche Daten dürfen nach dem jeweils anwendbaren Recht in den nationalen Melderegistern abgefragt werden?
- Wie sind personenbezogene Daten vor unbefugten Zugriffen zu schützen?
- Was muss ein Dienst datenschutzrechtlich leisten, wenn er personenbezogene Daten im Auftrag abfragt und weiterleitet?

Das Projekt RISER befindet sich mittlerweile in der dritten Phase: Nach erfolgreicher Marktevaluierung in Estland und Ungarn (RISERac) startete im September 2006 die Phase der Markteinführung (RISERid). Bis zum Jahr 2009 soll dabei der Dienst in weiteren Ländern der Europäischen Union schrittweise angeboten werden.

3.2.3 Staatliche Identifikationsnummern

3.2.3.1 Einleitung

Staatliche Stellen speichern personenbezogene Daten über Bürger in einer Vielzahl von Registern und sonstigen Datenbanken. Dabei werden dem einzelnen Bürger seitens der hoheitlichen Stellen sog. Identifikationsnummern („ID Numbers“) zugewiesen. Hierunter sind nicht nur reine Ziffernfolgen, sondern Kombinationen alphanumerischer Zeichen zu verstehen. Diese sollen die Unterscheidbarkeit aller Bürger voneinander gewährleisten und können dazu verwendet werden, die zu einer Person verfügbaren Datenbestände zu strukturieren.

Solche staatlichen Identifikationsnummern erleichtern die Verkettung personenbezogener Daten über einen Bürger, wobei umso mehr Verkettungen ermöglicht werden, je länger die jeweiligen Nummern gültig sind[175]. Werden ID-Nummern bereichsübergreifend verwendet, so stellt sich aus juristischer Sicht die Frage, ab wann es sich bei einer solchen Nummer um ein einheitliches Personenkennzeichen handelt, das dem Bundesverfassungsgericht zufolge verfassungsrechtlich unzulässig ist[176]. Aus Sicht des Datenschutzes unterscheidet man zudem zwischen sprechenden Nummern, aus denen bereits personenbezogene Daten wie das Geburtsdatum des Betroffenen abgelesen werden können, und nicht-sprechenden Nummern.

In Deutschland steht die Einführung zweier neuer bzw. erneuerter Identifikationsnummern unmittelbar bevor: Bei diesen handelt es sich um die steuerlich Identifikationsnummer und die neue Krankenversichertennummer. Eine weitere wichtige staatliche ID-Nummer ist die Rentenversicherungsnummer. Krankenversicherten- und Rentenversicherungsnummer werden nachfolgend unter dem Oberbegriff der Sozialversicherungsnummer vorgestellt. Anhand der jeweiligen Ausführungen soll verdeutlicht werden, in welchem Kontext und von wem die verschiedenen Nummern verwendet werden (dürfen) und welches Ausmaß an Verkettung sie demzufolge ermöglichen.

3.2.3.2 Sozialversicherungsnummer

3.2.3.2.1 Einführung

Eine Sozialversicherungsnummer ist eine ID-Nummer zur Identifizierung von Personen im Bereich des Sozialversicherungswesens. In einigen Staaten werden solche Nummern nicht nur für Zwecke der Sozialversicherung, sondern auch für andere Zwecke genutzt. So spielt die Sozialversicherungsnummer etwa in den Vereinigten Staaten eine herausragende Rolle[177]: Die dort verwendete Social Security Number (SSN) dient als universelles Personenidentifikationsmittel und wird nicht nur von vielen unterschiedlichen Behörden (u.a. den Finanzbehörden), sondern auch von privaten Unternehmen genutzt. Die Erkenntnis, dass mit einer solchen inflationären Nutzung einer staatlichen ID-

[175] Am „verkettungsfreundlichsten“ sind Nummern, die einer Person lebenslang zugeordnet werden.
[176] Hierzu siehe die Ausführungen im rechtlichen Abriss zu diesem Abschnitt unter 3.2.1.2.
[177] Gleiches gilt etwa auch für die Schweiz, in der die sog. AHV-Nummer von vielen unterschiedlichen hoheitlichen und privaten Stellen genutzt wird.

Nummer Risiken verbunden sind, hat sich mittlerweile auch in den USA durchgesetzt. Dort hat Präsident George W. Bush im Mai 2006 eine „Task Force Identitätsdiebstahl“ eingerichtet. Die Vorsitzenden dieser Task Force haben kürzlich ihren Strategieplan für den Kampf gegen Identitätsdiebstahl vorgestellt, der u.a. die Empfehlung enthält, die Verwendung der Sozialversicherungsnummer stark einzuschränken[178]. Die Angabe der Nummer werde nämlich sowohl von Behörden als auch von privaten Unternehmen viel zu häufig und in vielen Fällen ohne ausreichende Begründung verlangt. Darüber hinaus hat der Justizausschuss des US-amerikanischen Senats im Mai 2007 den Personal Data Privacy and Security Act of 2007 gebilligt, der nun dem US-Senat zur Abstimmung vorgelegt wird[179]. Der vom Justizausschuss gebilligte Entwurf enthält Vorschriften, die den Verkauf oder die Weitergabe von Sozialversicherungsdaten unter Strafe stellen. Damit soll erreicht werden, dass Unternehmen nicht mehr wie bisher ohne weiteres dieser Daten habhaft werden können, sondern nur unter bestimmten, gesetzlich definierten Voraussetzungen.

Anders als in den USA gibt es in Deutschland keine einheitliche Sozialversicherungsnummer für alle Versicherungszweige. Das Sozialgesetzbuch (SGB) V verbietet sogar ausdrücklich die Verwendung der Rentenversicherungsnummer als Krankenversichertennummer[180]. Hintergrund hierfür ist, dass das Bundesverfassungsgericht – wie bereits erwähnt – in seinem Volkszählungsurteil die Nutzung eines einheitlichen Personenkennzeichens für unzulässig erklärt hat. Nachfolgend werden die Rentenversicherungs- und die Krankenversichertennummer kurz vorgestellt.

3.2.3.2.2 Rentenversicherungsnummer

Die deutsche Rentenversicherungsnummer wird von den Rentenversicherungsträgern vergeben. Diese verwenden die Versicherungsnummer für die Bearbeitung aller ihrer Vorgänge. Von anderen Sozialversicherungsträgern wie den Krankenkassen oder den Pflegekassen darf die Nummer nur in bestimmten, gesetzlich klar definierten Fällen benutzt werden. Entsprechendes gilt für sonstige Behörden, Gerichte, Arbeitgeber und Dritte.

Anders als früher wird mittlerweile schon Neugeborenen eine Rentenversicherungsnummer zugeteilt[181], ein Sozialversicherungsausweis wird aber wie schon bisher erst mit der erstmaligen Aufnahme einer Erwerbstätigkeit erstellt.

Die Rentenversicherungsnummer einer Person besteht aus alphanumerischen Bauteilen und insgesamt 12 Stellen (Beispiel: 26030869M035). Sie ist eine sprechende Nummer und setzt sich wie folgt zusammen (siehe Tabelle 8):

Stelle	Inhalt / Bedeutung	Beispiel
1-2	Bereichsnummer des Rentenversicherungsträgers, der die Nummer vergeben hat	26
3-4	Geburtstag des Versicherten	03
5-6	Geburtsmonat des Versicherten	08
7-8	Geburtsjahr des Versicherten	69
9	Anfangsbuchstabe des Geburtsnamens des Versicherten	M
10-11	Seriennummer (00-49 = männlich, 50-99 = weiblich)	03

Tabelle 8: Aufbau der Rentenversicherungsnummer

[178] Hierzu vgl. die Meldung „Identitätsdiebstähle: USA wollen Strafrecht verschärfen“ bei heise online, abrufbar unter http://www.heise.de/newsticker/meldung/88845/ (letzter Zugriff im Oktober 2007).

[179] Vgl. die Meldung „Gesetz gegen Identitätsdiebstahl passiert US-Senatsausschuss“, abrufbar unter http://www.heise.de/newsticker/meldung/89341/ (letzter Zugriff im Oktober 2007).

[180] § 290 Abs. 1 Satz 3 SGB V.

[181] Dies ist dem Umstand geschuldet, dass die Krankenversicherungsnummer nunmehr auf der Basis der Rentenversicherungsnummer erstellt wird.

Die gesetzlichen Grundlagen für die Vergabe und den Aufbau der Rentenversicherungsnummer finden sich insbesondere in § 147 Abs. 2 Sozialgesetzbuch (SGB) VI[182].

3.2.3.2.3 Krankenversichertennummer

Bislang vergaben die einzelnen deutschen Krankenkassen Versicherungsnummern an ihre Versicherten. Im Zusammenhang mit der Einführung der elektronischen Gesundheitskarte, die nach gegenwärtigem Stand[183] wohl erst im Jahre 2010 erfolgen wird, werden die Versicherten auch neue Krankenversichertennummern erhalten[184]. Die Vergabe dieser Nummern erfolgt dabei nicht mehr durch die einzelnen Krankenkassen, sondern zentral durch die neu geschaffene „Vertrauensstelle Krankenversichertennummer".

Die krankenkasseninterne Umstellung auf die neuen Nummern ist bereits Ende März 2006 weitgehend abgeschlossen worden. Die Versicherten werden die Nummern allerdings erst zusammen mit ihren neuen elektronischen Gesundheitskarten erhalten. Die neuen Nummern sind nicht-sprechend, bestehen aus 20 Ziffern und setzen sich aus einem veränderbaren[185] und einem unveränderbaren, also lebenslang gültigen Teil[186] zusammen (siehe Tabelle 9):

Stelle	Inhalt / Bedeutung	Beispiel
1-10	unveränderbarer Teil (zum Versicherten gehörig)	1234567890
11-19	veränderbarer Teil (zur Krankenkasse gehörig)	123456789
20	Prüfziffer	1

Tabelle 9: Aufbau der neuen Krankenversichertennummer

Die gesetzlichen Grundlagen für die Einführung dieses einheitlichen Systems der Krankenversichertennummer wurden durch das GKV-Modernisierungsgesetz 2003 geschaffen und finden sich insbesondere in § 290 Sozialgesetzbuch (SGB) V in seiner seitdem gültigen Fassung[187].

3.2.3.2.4 Verkettung mittels Renten- und Krankenversichertennummer

Wie schon bisher darf die Rentenversicherungsnummer aus Datenschutzgründen auch weiterhin nicht als Krankenversichertennummer verwendet werden[188]. Durch das Verbot der Einführung einer einheitlichen Sozialversicherungsnummer soll der Gefahr begegnet werden, dass eine solche Nummer Schritt für Schritt zu einem einheitlichen Personenkennzeichen ausgebaut werden könnte.

Allerdings darf die Rentenversicherungsnummer seit der GKV-Reform 2003 für die Generierung der Krankenversichertennummer verwendet werden. Diese wird nunmehr auf Basis der Rentenversicherungsnummer und mit Hilfe eines Verschlüsselungsverfahrens erzeugt. Dieses Verfahren ist allerdings nur dann zulässig, wenn nach dem Stand von Wissenschaft und Technik sichergestellt ist, dass nach Vergabe der Krankenversichertennummer von keiner der beiden Nummern auf die andere rückgeschlossen werden kann[189].

[182] Einzelheiten enthält § 2 der Verordnung über die Versicherungsnummer, die Kontoführung und den Versicherungsverlauf in der gesetzlichen Rentenversicherung (VKVV).
[183] Hierzu vgl. die Meldung „Bericht: Elektronische Gesundheitskarte verzögert sich", abrufbar unter http://www.heise.de/newsticker/meldung/88260/ (letzter Zugriff im Oktober 2007).
[184] Einzelheiten hierzu finden sich unter https://kvnummer.gkvnet.de/ (letzter Zugriff im Oktober 2007).
[185] Dieser veränderbare Teil enthält das Institutionszeichen der jeweiligen Krankenkasse und ändert sich demzufolge bei jedem Krankenkassenwechsel.
[186] Bisher bekamen die Versicherten hingegen bei einem jeden Krankenkassenwechsel eine neue Versichertennummer.
[187] Aufgrund dieser Vorschrift haben die Spitzenverbände der Krankenkassen gemeinsame Richtlinien erlassen, die den Aufbau und das Verfahren der Vergabe der neuen Nummer im Einzelnen regeln.
[188] Dies regelt § 290 Abs. 1 S. 4 Sozialgesetzbuch (SGB) V.
[189] § 290 Abs. 1 S. 5 SGB V.

Mögliche Verkettungen mittels der Renten- und der neuen Krankenversichertennummer werden aus rechtlicher Sicht durch den bereits mehrfach erwähnten Umstand beschränkt, dass beide Nummern gerade nicht als einheitliche Sozialversicherungsnummer verwendet werden dürfen. Vielmehr ist die Nutzung der Krankenversichertennummer auf den Bereich der gesetzlichen Krankenversicherung beschränkt. Die Rentenversicherungsnummer darf hingegen grundsätzlich nur von den Trägern der gesetzlichen Rentenversicherung verwendet werden[190].

3.2.3.3 Steuerliche Identifikationsnummer

3.2.3.3.1 Allgemeines

Mit der steuerlichen Identifikationsnummer wurde ab Juli 2007[191] eine weitere neue staatliche Identifikationsnummer eingeführt. Bei dieser handelt es sich um ein einheitliches und unveränderliches Identifikationsmerkmal für natürliche Personen, das jedem Steuerpflichtigen[192] zum Zwecke der eindeutigen Identifizierung in Besteuerungsverfahren zugeteilt wird und bei Anträgen, Erklärungen oder Mitteilungen gegenüber den Finanzbehörden angegeben werden muss[193]. Damit sind Stellen wie z.B. Banken, Arbeitgeber oder Sozialbehörden, die mit den Finanzämtern hinsichtlich konkreter Steuerfälle kommunizieren, dazu verpflichtet, diese Nummer zu speichern und gegenüber den zuständigen Finanzbehörden zu verwenden.

Vergeben wird die steuerliche Identifikationsnummer vom Bundeszentralamt für Steuern (BZSt)[194]. Dieses speichert die Nummer zusammen mit weiteren Daten über den Steuerpflichtigen – wie Name, Tag und Ort der Geburt, Geschlecht sowie gegenwärtige Anschrift –, die ihm zuvor von den kommunalen Meldebehörden übermittelt werden. Im Gegenzug übermittelt das Bundeszentralamt die zugeteilte Identifikationsnummer zwecks Speicherung im Melderegister an die Meldebehörden.

Die steuerliche Identifikationsnummer besteht aus einer Folge von 11 Ziffern, die nicht aus anderen Daten über den Steuerpflichtigen gebildet oder abgeleitet werden dürfen. Es handelt sich bei ihr also um eine nicht-sprechende Nummer (siehe Tabelle 10):

Stelle	Inhalt / Bedeutung	Beispiel
1-10	zehnstellige Zahl	1234567890
11	Prüfziffer	1

Tabelle 10: Aufbau der steuerlichen Identifikationsnummer

Die Rechtsgrundlage für die Einführung der steuerlichen Identifikationsnummer wurde durch das Steueränderungsgesetz 2003 geschaffen und findet sich in §§ 139a ff. der Abgabenordnung (AO)[195].

[190] Andere Sozialversicherungsträger sowie Behörden und Unternehmen dürfen die Nummer nur in bestimmten, gesetzlich klar definierten Fällen nutzen.

[191] Die Ausgabe der Nummern an die Bürger verzögert sich etwas und wird voraussichtlich erst im Laufe des Jahres 2008 geschehen.

[192] Künftig werden auch alle Neugeborenen eine solche steuerliche Identifikationsnummer erhalten, die erst 20 Jahre nach dem Tod endgültig gelöscht werden soll.

[193] Über die steuerliche Identifikationsnummer hinaus erhalten wirtschaftlich tätige natürliche Personen auch noch eine sog. Wirtschafts-Identifikationsnummer. Gleiches gilt auch für juristische Personen und Personenvereinigungen. Auf die Wirtschafts-Identifikationsnummer soll an dieser Stelle aber nicht weiter eingegangen werden.

[194] Näheres zu dieser zum 01.01.2006 als Nachfolgebehörde des Bundesamtes für Finanzen (BAF) eingerichteten Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Finanzen (BMF) findet sich auf deren Internetpräsenz unter http://www.bzst.bund.de/ (letzter Zugriff im Oktober 2007).

[195] Im Dezember 2006 ist darüber hinaus auch die Steueridentifikationsnummerverordnung (StIdV) in Kraft getreten, die Einzelheiten zur Vergabe der Identifikationsnummern regelt.

3.2.3.3.2 Steuerliche Identifikationsnummer und Verkettung

Nach § 139b AO darf die steuerliche Identifikationsnummer nur für steuerliche Zwecke erhoben und verwendet werden. Ein wesentliches Ziel dieser Vorschrift besteht darin, die Verwendung der Nummer als einheitliches Personenkennzeichen in Verwaltung und Wirtschaft zu verhindern. Konsequenterweise dürfen öffentliche oder private Stellen ihre Dateien auch nur insoweit nach der Identifikationsnummer ordnen oder für den Zugriff erschließen, als dies für regelmäßige Datenübermittlungen zwischen ihnen und den Finanzbehörden erforderlich ist[196].

Nach geltendem Recht darf die steuerliche Identifikationsnummer also nur zu Zwecken des Besteuerungsverfahrens verwendet und damit auch nur zur Verkettung der in diesem Zusammenhang anfallenden personenbezogenen Daten eingesetzt werden. Solange diese Zweckbestimmung auch zukünftig durch gesetzliche Regelungen gewährleistet wird, dürfte die Verwendung der steuerlichen Identifikationsnummer im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts zur Unzulässigkeit eines einheitlichen Personenkennzeichens als unbedenklich einzustufen sein.

Allerdings gibt es Anzeichen dafür, dass die Verwendung dieser Nummer sukzessive ausgeweitet werden könnte. So soll die Nummer nicht nur bei den zuständigen Finanzbehörden und beim Bundeszentralamt für Steuern, sondern auch in den kommunalen Melderegistern gespeichert werden[197]. Die beim Bundeszentralamt für Steuern geführte Datenbank wird zudem auch weitere Daten wie Name und Adresse enthalten, die durch Datenübermittlungen der Meldebehörden stets auf dem aktuellen Stand gehalten werden sollen. Wie bereits an anderer Stelle erwähnt[198], plant die gegenwärtige Bundesregierung schließlich eine Zentralisierung des Meldewesens, weshalb es in naher Zukunft zum Aufbau eines zentralen Melderegisters für ganz Deutschland kommen dürfte. Insofern ist zu vermuten, dass die steuerliche Identifikationsnummer dann nicht mehr nur in den kommunalen, sondern auch in diesem zentralen Melderegister gespeichert werden wird.

Dass ein zentrales Melderegister mit einer zentralen Melderegisternummer (ZMR) allerdings nicht zwangsläufig dazu führen muss, dass diese Identifikationsnummer als einheitliches Personenkennzeichen verwendet wird, zeigt das Beispiel Österreichs. Dort ist mit dem E-Government-Gesetz 2004 die Entscheidung dafür gefallen, im Bereich der elektronischen Verwaltung anstelle einer einheitlichen ID-Nummer verschiedene bereichsspezifische Personenkennzeichen (bPK) zu verwenden. Dieses sog. Konzept Bürgerkarte[199] verhindert die Entstehung eines einheitlichen Personenkennzeichens im Bereich des E-Government und wirkt damit umfangreichen Verkettungen und der Erstellung von Profilen über die österreichischen Bürger entgegen.

3.2.3.4 Fazit

Mittels staatlicher Identifikationsnummern können personenbezogene Daten über Bürger einfach miteinander verkettet werden. Bislang werden in Deutschland ausschließlich sektorbezogene Identifikationsnummern verwendet. Um eine solche bereichsspezifische Nummer handelt es sich auch bei der neuen Krankenversichertennummer.

Etwas anders stellt sich die Situation hinsichtlich der künftigen steuerlichen Identifikationsnummer dar. Zwar darf sie nach geltendem Recht lediglich für Zwecke des Besteuerungsverfahrens verwendet werden, allerdings lassen es die geplante Speicherung der Nummer in den kommunalen Melderegistern und die bevorstehende Zentralisierung des Meldewesens als möglich erscheinen, dass sie sukzessive zu einem einheitlichen Personenkennzeichen ausgebaut werden könnte. Sollte dies tatsächlich so kommen, so wäre diese Entwicklung am verfassungsgerichtlichen Verbot eines einheitlichen Personenkennzeichens zu messen.

---

[196] § 139b Abs. 2 S. 2 Nr. 2 AO. Hierbei handelt es sich um zwingendes Recht, das also nicht durch Vertragsbestimmungen oder Einwilligungserklärungen abbedungen werden kann. Nichtöffentliche Stellen, die gegen diese Vorschrift verstoßen, begehen nach § 383a AO eine Ordnungswidrigkeit, die mit einer Geldbuße bis zu 10.000 EUR geahndet werden kann.

[197] Vgl. § 2 Abs. 2 Nr. 7 MRRG.

[198] Siehe oben im Abschnitt 3.2.2 zu staatlichen Registern.

[199] Hierzu ausführlich [Kotschy 2006] sowie [Meints/Hansen 2006, S. 90].

3.2.4 Staatliche Identitätsdokumente

3.2.4.1 Typen von Identitätsdokumenten

In der Bundesrepublik Deutschland werden derzeit zwei grundsätzliche Typen von Identitätsdokumenten verwendet:

1. papiergebundene Dokumente, die teilweise mit maschinenlesbarer Zone ausgestattet sind;
2. elektronische Identitätsdokumente.

Der aktuelle Personalausweis gehört zur ersten Gruppe; elektronische Signaturkarten, der Reisepass und der zukünftige Personalausweis gehören der zweiten Gruppe an.

3.2.4.2 Reisepass

Zweck des Reisepasses ist es, Bürger der Bundesrepublik bei Auslandsreisen zu identifizieren. Dabei sind Pässe nicht nur an Grenzübergängen, sondern vielfach auch an anderen Orten, z.B. in Hotels, vorzuzeigen oder für einen begrenzten Zeitraum (bis zu zwei Stunden in Italien, bis zu acht Stunden in der Slowakei) sogar abzugeben.[200] Rechtsgrundlage für die (technische) Implementierung des Reisepasses sind die EU-Verordnung 2252/2004 und das bundesdeutsche Passgesetz – nach beiden sind die Spezifikationen der International Civil Aviation Organisation (ICAO), die insbesondere im Dokument 9303 über maschinenlesbare Reisedokumente zu finden sind, zu berücksichtigen.

Herzstück des Reisepasses ist eine mit Polycarbonat laminierte Karte, die die persönlichen Daten, aber auch die Nationalität des Passinhabers und die ausstellende Behörde beinhaltet. Diese Karte enthält auch eine mittels optischer Scanner und Zeichenerkennung lesbare Zone („machine readable zone“, MRZ). Diese beinhaltet neben dem Namen des Passinhabers auch die Passnummer, das Geburtsdatum und das Ablaufdatum der Gültigkeit des Passes.

Seit November 2005 sind neu ausgestellte Reisepässe mit einem RFID-Chip ausgestattet, der die Daten des Passinhabers auch digital speichert. Zusätzlich wird im RFID-Chip ein digitales Gesichtsbild gespeichert, das für biometrische Gesichtserkennung genutzt werden kann[201]. Ab November 2007 sollen neben weiteren Daten auch die Bilder zweier Fingerabdrücke digital gespeichert werden.

Üblicherweise wird im Ausland die Passnummer in Hotels für jede Übernachtung zusammen mit weiteren Daten (meist Name, Geburtsdatum und Wohnort) gespeichert. Da die Passnummer eindeutig ist, erlaubt sie eine Verkettung von Datensätzen, die während einer Reise im Ausland erhoben und gespeichert wurden. Der RFID-Chip ermöglicht unter bestimmten Voraussetzungen (u.a. Bekanntsein der Daten der MRZ, Einsatz zweier oder mehrerer Leser an räumlichen Engestellen wie z.B. Türdurchgängen etc.) das Verfolgen (Tracken) einzelner Personen und kleiner Gruppen.[202] Mit Hilfe von Videoüberwachungstechnik kann auch das digitale Passbild als biometrische Referenz zum Verfolgen von Personen verwendet werden, auch wenn diese Technik gegenwärtig noch nicht sehr zuverlässig zu sein scheint.[203] Die jetzige Realisierung des Reisepasses mit RFID-Chip begünstigt die Möglichkeit, Bewegungsprofile der Reisenden zu erstellen.

Über den Namen und das Geburtsdatum ist die Verkettung weiterer Daten, z.B. hinsichtlich im Ausland getätigter Banktransaktionen, möglich.

---

[200] Vgl. [Meints/Hansen 2006].

[201] Siehe http://www.bsi.de/fachthem/epass/merkmale.htm und http://www.bsi.de/fachthem/epass/Sicherheitsmerkmale.pdf (letzter Zugriff jeweils im Oktober 2007).

[202] [Kosta et al. 2007].

[203] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen zum geplanten Einsatz in Lichtbilddokumenten – BioP I“, Bonn 2004, abrufbar unter http://www.bsi.de/literat/studien/biop/biopabschluss.pdf (letzter Zugriff im Oktober 2007).

3.2.4.3 Personalausweis

Zweck des Personalausweises ist es, Bürger in der Bundesrepublik gegenüber staatlichen Stellen zu identifizieren. Er wird darüber hinaus aber auch im wirtschaftlichen Umfeld verwendet, um etwa das Alter des Ausweisinhabers zu überprüfen. Rechtsgrundlage ist das Personalausweisgesetz.

Der Personalausweis ist eine mit Polycarbonat laminierte Karte, deren Informationen der Karte im Reisepass vergleichbar sind. Ergänzend wird im Personalausweis die aktuelle Wohnadresse durch die zuständige Behörde vermerkt. Der Personalausweis verfügt ebenfalls über eine maschinenlesbare Zone und eine eindeutige Ausweisnummer, die auch im Melderegister gespeichert ist. Wird bei Ausweiskontrollen die Ausweisnummer gespeichert, so ist eine Verkettung der Kontrollereignisse miteinander und mit den Melderegisterdaten möglich.

Zukünftig soll der Personalausweis die technischen Merkmale des Reisepasses (RFID-Chip und biometrische Referenzdaten) sowie einen Kontakt-Chip für die Speicherung von Schlüsseln und Zertifikate für elektronische Signaturen beinhalten [Engel 2006]. Damit werden im Zusammenhang mit dem Personalausweis zusätzlich auch die bei diesen Dokumenten genannten Möglichkeiten zur Verkettung bestehen.

3.2.4.4 Elektronische Signaturkarten

Zweck elektronischer Signaturkarten ist die Speicherung privater Schlüssel und Zertifikate, die für die Erstellung elektronischer Signaturen benötigt werden. Rechtsgrundlage sind das Signaturgesetz und die Signaturverordnung. Die Signaturkarten werden in der Bundesrepublik von privaten Dienstleistungsanbietern auf Basis gesetzlicher Vorgaben angeboten. Die dahinter liegende Public-Key-Infrastruktur (PKI) zur Online-Überprüfung der Daten auf der Signaturkarte wird ebenfalls von Privatunternehmen bereitgestellt. Die PKI wird durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert.

Bei jeder elektronischen Signatur wird das Zertifikat (Format: X.509v3) des Inhabers der Signaturkarte gespeichert. Neben einer eindeutigen Seriennummer (Zertifikatsnummer) beinhaltet das Zertifikat den Namen des Inhabers der Signaturkarte und das Ablaufdatum der Gültigkeit des auf der Signaturkarte gespeicherten privaten Schlüssels.

Eine Verkettung geleisteter elektronischer Signaturen einer Person ist über die in jedem Falle mitgespeicherte Nummer in den Zertifikaten möglich. Die Verkettung könnten Nutzer durch die Verwendung mehrerer pseudonymer Signaturkarten auf die jeweiligen Einsatzbereiche einschränken. Der Einsatz pseudonymer Signaturen ist in der Bundesrepublik jedoch beim E-Government gesetzlich eingeschränkt [Hornung 2006].

3.2.5 E-Government

3.2.5.1 Einleitung

Der Terminus E-Government setzt sich aus den Begriffen „electronic“ (engl. für elektronisch, rechnergestützt) und „Government“ (engl. für Verwaltung, Regierung) zusammen. Wie der Name schon sagt, geht es bei E-Government darum, Aufgaben der öffentlichen Verwaltung mittels moderner Informations- und Kommunikationstechnologien (IuK-Technologien) zu erfüllen. Prinzipiell werden insoweit also alle verfügbaren IuK-Technologien umfasst – allerdings ist anzumerken, dass sich E-Government zum gegenwärtigen Zeitpunkt noch überwiegend auf den kombinierten Einsatz von World Wide Web (WWW), elektronischer Post (E-Mail), elektronischen Datenaustausch (EDI) und hierauf abgestimmte Datenbanksysteme beschränkt. Das Spektrum der via E-Government angebotenen Dienstleistungen reicht von reinen Informationsdiensten über verschiedene Kommunikationsdienste (wie z.B. E-Mail)

bis hin zu sog. Transaktionsdiensten, die eine für beide Seiten verbindliche und möglichst vollständige elektronische Abwicklung von Verwaltungsaufgaben ermöglichen sollen.[204]

Es gibt zahlreiche Versuche einer exakten Definition des Begriffs E-Government, von denen an dieser Stelle (exemplarisch) nur die sog. Speyerer Definition[205] vorgestellt werden soll. Nach dieser ist unter E-Government „die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien“ zu verstehen. Der Begriff des E-Government im Sinne dieser Definition umfasst neben der kommunalen, der Landes- und der nationalen auch die supranationale und globale Ebene sowie auf jeder dieser Ebenen jeweils den kompletten öffentlichen Sektor, also neben der Exekutive auch die Legislative, die Judikative und alle öffentlichen Unternehmen.

Weiterhin kann nach der Speyerer Definition beim E-Government auch danach unterschieden werden, welche Personen bzw. Organisationen jeweils involviert sind: Hier ist zwischen verwaltungsinternen Prozessen (Government-to-Government, G2G) und solchen, die das Verhältnis von Verwaltung und privaten Stellen betreffen, zu differenzieren. Bei Letzteren unterscheidet man wiederum zwischen dem Verhältnis Verwaltung-Bürger (Government-to-Citizen, G2C), Verwaltung-Wirtschaft (Government-to-Business, G2B) und Verwaltung-Nichtregierungsorganisation (Government-to-Non-Governmental Organization, G2N).[206]

Schließlich ist anzumerken, dass E-Government oft als Oberbegriff für die verschiedenen Teilbereiche E-Administration (E-Government im engeren Sinne), E-Democracy (betrifft die politische Teilhabe von Bürgern) und E-Justice (betrifft den Bereich der Judikative) verwendet wird.

3.2.5.2 Wichtige aktuelle E-Government-Initiativen in Deutschland

Im Juni 2003 wurde die gemeinsame E-Government-Strategie von Bund, Ländern und Kommunen mit dem Namen Deutschland-Online[207] gestartet. Diese verbindet die E-Government-Initiative des Bundes[208], die verschiedenen E-Government-Programme der Länder und die E-Government-Projekte der Kommunen. Zur Vertiefung der Kooperation im Rahmen dieser gemeinsamen Strategie wurde im Juni 2006 der Aktionsplan Deutschland-Online[209] beschlossen. Das Ziel dieses Aktionsplans besteht vor allem im Aufbau eines gemeinsamen, integrierten und sicheren Kommunikationsnetzes für die Verwaltung in Bund, Ländern und Gemeinden. Dabei wurden zunächst fünf Vorhaben bestimmt, die priorisiert umgesetzt werden sollen. Zwei der Vorhaben betreffen die Bereiche IT-Infrastruktur und Standardisierung von Datenaustauschformaten[210]. Die drei weiteren Vorhaben, nämlich Kfz-Wesen, Personenstandswesen und Meldewesen, haben hingegen bestimmte Fachverfahren zum Gegenstand.

Auf Ebene des Bundes wurde im Rahmen der E-Government-Initiative BundOnline 2005 bereits im Jahr 2000 damit begonnen, Dienstleistungen der Bundesverwaltung online zu stellen. Ziel dieser Initiative war es, alle internetfähigen Dienstleistungen von Bundesbehörden online anzubieten. Das Ergebnis von BundOnline 2005 bestand darin, dass bis zum Abschluss der Initiative am 31. Dezember 2005 etwa 440 Informations-, Kommunikations- und Transaktionsdienstleistungen des

[204] Einzelheiten hierzu finden sich etwa in den Handlungsempfehlungen „Datenschutzgerechtes eGovernment“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, S. 6 f. Diese Empfehlungen sind abrufbar unter http://cdl.niedersachsen.de/blob/images/C1358174_L20.pdf (letzter Zugriff im Oktober 2007). In den Handlungsempfehlungen wird nicht nur zwischen Informations-, Kommunikations- und Transaktionsdiensten unterschieden, sondern darüber hinaus auch noch der Begriff des E-Verwaltungsverfahrens (elektronisches Verwaltungsverfahren) eingeführt, der einen Unterfall elektronischer Transaktionsdienste bezeichnet. Charakteristisch für das E-Verwaltungsverfahren ist, dass es sich nicht auf die Durchführung reiner Transaktion beschränkt, sondern auch das Vor- und Umfeld von Verwaltungsentscheidungen umfasst.

[205] Die vollständige Speyerer Definition ist abrufbar unter http://foev.dhv-speyer.de/ruvii/Sp-EGov.pdf (letzter Zugriff im Oktober 2007).

[206] Alle genannten Konstellationen sollen dabei auch den jeweils umgekehrten Informationsfluss beinhalten, weshalb etwa G2C gleichzeitig auch für C2G stehen soll.

[207] http://www.deutschland-online.de/ (letzter Zugriff im Oktober 2007).

[208] Hierzu sogleich.

[209] Dieser ist unter http://www.deutschland-online.de/ abrufbar (letzter Zugriff im Oktober 2007).

Bundes online verfügbar gemacht wurden[211]. Die verschiedenen Dienstleistungen können dabei sowohl über die Website der jeweiligen Bundesbehörde als auch über das zentrale Verwaltungsportal des Bundes unter http://www.bund.de/ aufgerufen werden.

Ausgehend von den bereits mit Deutschland-Online und BundOnline 2005 gemachten Erfahrungen hat die Bundesregierung im September 2006 das Programm E-Government 2.0[212] beschlossen, das durch alle Bundesressorts umgesetzt werden soll. Im Rahmen dieses Programms sollen verschiedene Handlungsfelder, die die Bundesregierung als besonders wichtig einstuft, bis zum Jahr 2010 gezielt ausgebaut werden[213]. So besteht etwa das Ziel des Handlungsfelds Identifizierung in der Einführung eines elektronischen Personalausweises und in der Erarbeitung von E-Identity-Konzepten, wohingegen im Rahmen des Handlungsfelds Kommunikation eine sichere Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltungen geschaffen werden soll. Letztere soll etwa durch die Implementierung zertifizierter Bürgerportale, die u.a. mit sicheren elektronischen Postfächern und elektronischen Meldeadressen ausgestattet sind, erreicht werden.[214]

3.2.5.3 E-Government und Verkettung

Je mehr Dienstleistungen unterschiedlicher Behörden ein Bürger online nachfragt, umso mehr seiner verschiedenen digitalen Teilidentitäten (z.B. als Steuer- oder Sozialversicherungspflichtiger) sind betroffen und umso mehr digitale Daten über ihn fallen im Rahmen des E-Government an. Dabei ist es technisch grundsätzlich möglich, alle diese Identitäten und die dazugehörigen Daten miteinander zu verketten. Verkettet werden kann etwa mit Hilfe von Cookies, staatlichen Identifikationsnummern oder Informationen wie Name und Geburtsdatum. Dies ist dann besonders leicht, wenn dem Bürger Verwaltungsdienstleistungen unterschiedlicher Behörden über eine zentrale Stelle – wie beispielsweise ein umfassendes Bürgerportal, über das Bürger auf eine Vielzahl von Dienstleistungen aus unterschiedlichen Bereichen der Verwaltung zugreifen können, – angeboten werden. In solchen Konstellationen ist es besonders wichtig, dass eine strikte Wahrung des Zweckbindungsgrundsatzes sichergestellt wird und willkürliche Verkettungen verschiedener Teilidentitäten unterbunden werden. Ist dies nicht gewährleistet, besteht die Gefahr, dass unterschiedliche Identitäten und die dazugehörigen Daten zur Generierung umfassender Persönlichkeitsprofile über den jeweiligen Bürger verwendet werden.

Für viele Verwaltungsdienstleistungen gilt ein Schriftformerfordernis, d.h., der Bürger muss ein schriftliches Dokument eigenhändig unterschreiben[215]. Allerdings kann eine durch Rechtsvorschrift vorgeschriebene Schriftform grundsätzlich durch die sog. elektronische Form ersetzt werden.[216] In diesem Fall muss das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen werden.[217] Möchte die Verwaltung dem Bürger also möglichst viele Dienstleistungen via E-Government anbieten, so lässt sich dies nach geltendem Recht nur dann realisieren,

[210] Als Ergebnis der bisherigen Standardisierungsbemühungen ist primär der OSCI-Standard (Online Services Computer Interface) zu nennen. Das sog. OSCI-Transport-Protokoll soll die Integrität, Authentizität, Vertraulichkeit und Nachvollziehbarkeit bei der Übermittlung von Nachrichten sicherstellen und stellt folglich die Spezifikation eines sicheren Transportprotokolls dar. Außerdem wurden durch die OSCI-Leitstelle mittlerweile auch schon einige (XML-basierte) Spezifikationen von Inhaltsdaten wie beispielsweise XMeld oder XJustiz standardisiert. Zum Thema OSCI vgl. auch die entsprechende Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die unter https://www.datenschutzzentrum.de/material/themen/presse/20051216-dsbk-osci.htm abgerufen werden kann (letzter Zugriff im Oktober 2007).

[211] Abschlussbericht BundOnline 2005, S. 3, abrufbar unter http://www.kbst.bund.de/Content/Egov/Initiativen/Bol/bol.html (letzter Zugriff im Oktober 2007).

[212] Informationen hierzu finden sich etwa unter http://www.staat-modern.de/E-Government/-,13073/E-Government-2.0.htm (letzter Zugriff im Oktober 2007).

[213] Im Einzelnen handelt es sich um die Handlungsfelder Portfolio, Prozessketten, Identifizierung und Kommunikation.

[214] Einzelheiten zu allen Handlungsfeldern findet sich in der Broschüre E-Government 2.0, die abrufbar ist unter http://www.staat-modern.de/Anlage/original_1070438/E-Governemt-2.0-Das-Programm-des-Bundes.pdf (letzter Zugriff im Oktober 2007).

[215] [Thome 2005] nennt insoweit einen Wert von 31 % aller Fälle und beruft sich insoweit auf eine Online-Umfrage des Lehrstuhls für Wirtschaftsinformatik der Universität Würzburg aus dem Jahre 2005.

[216] Vgl. §§ 3a Abs.2 S. 1 VwVfG, 36a Abs. 2 S. 1 SGB I, 87a Abs. 3 S. 1 AO.

wenn qualifizierte digitale Signaturen zum Einsatz kommen. In diesem Zusammenhang ist daran zu erinnern, dass Verkettungen auch anhand der jeweiligen Zertifikatsinformationen vorgenommen werden können. Insoweit birgt die Verwendung qualifizierter Signaturen im E-Government also auch das Risiko einer Verkettung einzelner Dokumente anhand eines übergreifend verwendeten Zertifikats.

Eine bereichsübergreifende Verkettung wird noch zusätzlich erleichtert, wenn seitens der Verwaltung ein Personenkennzeichen (etwa in Gestalt einer Identifikationsnummer) verwendet wird. An dieser Stelle ist noch einmal darauf hinzuweisen, dass in Deutschland gegenwärtig ausschließlich bereichsspezifische Identifikationsnummern verwendet werden, aber nicht ausgeschlossen werden kann, dass insbesondere die ab Juli 2007 vergebene steuerliche Identifikationsnummer zu einem universellen Personenkennzeichen ausgebaut wird.[218] Auch in Österreich gibt es verschiedene staatliche Identifikationsnummern – wie etwa die Melderegisternummer (sog. ZMR-Zahl) oder die Sozialversicherungsnummer –, die das Potenzial dazu haben, zu einem universellen Personenkennzeichen weiterentwickelt zu werden. Dort hat der Gesetzgeber jedoch mit dem Bürgerkartenkonzept für den Bereich des E-Government einen Ansatz gewählt, der zwar eine eindeutige Identifizierung und Authentisierung eines Bürgers ermöglicht, aber aus Datenschutzgründen statt eines universellen verschiedene bereichsspezifische Personenkennzeichen verwendet.[219] Die Rechtsgrundlage hierfür findet sich im Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz 2004[220]). Mit diesem Gesetz hat der österreichische Gesetzgeber auf unterschiedliche juristische Herausforderungen von E-Government reagiert.

Wie bereits beschrieben, stellt ein anonymes oder pseudonymes Auftreten für den jeweils Betroffenen ein wichtiges Instrument zur Steuerung von Verkettung dar. Im Bereich des E-Government sind diesen Möglichkeiten allerdings enge Grenzen gesetzt.[221]

Dies gilt zunächst für die Möglichkeit einer Verwendung von Pseudonymen: Soll etwa die Schriftform durch die elektronische Form ersetzt werden, so ist zu beachten, dass zur Signierung gem. § 7 Abs. 1 Satz 1 Nr. 1 SigG zwar grundsätzlich auch ein Pseudonym verwendet werden kann, dies jedoch im Bereich des E-Government nur eingeschränkt möglich ist. Nach §§ 3a Abs.2 Satz 3 Verwaltungsverfahrensgesetz (VwVfG), 36a Abs. 2 Satz 3 Sozialgesetzbuch I (SGB I) ist die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, unzulässig. Dies bedeutet konkret, dass nur ein solches Pseudonym verwendet werden darf, anhand dessen die ein Dokument empfangende Behörde den Bürger selbst identifizieren kann.[222] Im Bereich der Finanzverwaltung ist nach § 87a Abs. 3 Satz 3 Abgabenordnung (AO) die Signierung mit einem Pseudonym sogar generell unzulässig. Insgesamt lässt sich konstatieren, dass Bürger bei der Nutzung von E-Government-Angeboten in den meisten Konstellationen ihre Identität offenlegen müssen[223] und damit für den Bürger ein Auftreten unter einem Pseudonym regelmäßig nicht möglich ist.

Da die Offenlegung der Identität Voraussetzung für eine Vielzahl von E-Government-Diensten ist, scheidet auch ein anonymes Auftreten des Bürgers in den meisten Konstellationen aus. Möglich ist ein solches für den Bürger allerdings etwa dann, wenn er reine Informationsdienste in Anspruch nimmt oder generelle Anfragen stellt, bei deren Beantwortung es auf seine Identität nicht ankommt. Gleiches gilt auch für die – einfache – Online-Melderegisterauskunft gem. § 21 Abs. 1a Melderechtsrahmengesetz (MRRG), da diese an keinerlei Voraussetzungen in der Person des Antragstellers gebunden ist und deshalb dessen Identität für die Auskunftserteilung keine Rolle spielt.[224] Insoweit ist

[217] §§ 3a Abs. 2 S. 2 VwVfG, 36a Abs. 2 S. 2 SGB I, 87a Abs. 3 S. 1 AO. Der Begriff der qualifizierten elektronischen Signatur wird in § 2 Nr. 3 des Signaturgesetzes (SigG) definiert.

[218] Zu dieser siehe bereits Abschnitt 3.2.3.3.

[219] Hierzu ausführlich [Kotschy 2006, S. 201] sowie [Meints/Hansen 2006, S. 90].

[220] Abrufbar unter http://www.cio.gv.at/egovernment/law/ (letzter Zugriff im Oktober 2007).

[221] Einzelheiten zu dieser Thematik finden sich bei [Gundermann 2003].

[222] Es genügt also nicht, wenn die Identifizierung zwar dem Zertifizierungsdiensteanbieter, jedoch nicht der Verwaltung möglich ist, da die Verwaltung keinen generellen Auskunftsanspruch gegenüber dem Zertifizierungsdiensteanbieter hat. Hierzu vgl. E-Government-Handbuch des BSI, Kapitel „Rechtliche Rahmenbedingungen“, S. 62. Dieses ist online abrufbar unter http://www.bsi.bund.de/fachthem/egov/download/2_Recht.pdf (letzter Zugriff im Oktober 2007).

[223] Zu Problemen der Identifizierung im Bereich des E-Government vgl. [Roßnagel 2002].

[224] Hierzu vgl. [Gundermann 2003, S. 286].

allerdings zu beachten, dass für die Erteilung der Melderegisterauskunft seitens der Kommunen regelmäßig ein Entgelt verlangt wird. Hieraus folgt, dass ein anonymes Auftreten des Bürgers in diesen Fällen zusätzlich davon abhängig ist, dass ihm auch eine anonyme Zahlungsmöglichkeit[225] eingeräumt wird.

E-Government-Anwendungen wie etwa Bürgerportale oder andere Angebote via World Wide Web sind rechtlich als Telemedien im Sinne des Telemediengesetzes (TMG) zu qualifizieren. Sofern es sich bei einer Anwendung um einen solchen Telemediendienst handelt, hat die Verwaltung als Anbieter des jeweiligen Dienstes also die Regelungen des TMG zu beachten. Zu den Pflichten, denen sie insoweit genügen muss, gehört neben der Verpflichtung zur Anbieterkennzeichnung des § 5 Abs. 1 TMG insbesondere auch die Unterrichtungspflicht des § 13 Abs. 1 TMG. Hiernach hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten in allgemein verständlicher Form zu unterrichten.[226] Gleiches gilt für ein automatisiertes Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet. Hierdurch wird also klargestellt, dass sich die Unterrichtungspflicht auch auf automatisierte Verfahren bezieht, die eine Verarbeitung von Daten ermöglichen, bei denen der Personenbezug erst zu einem späteren Zeitpunkt hergestellt werden kann. In beiden Fällen muss der Inhalt der Unterrichtung für den Nutzer jederzeit abrufbar sein.

Genügt werden kann den eben genannten Pflichten durch die Platzierung einer Datenschutzerklärung[227] auf der jeweiligen Website.[228] Die Datenschutzerklärung sollte leicht auffindbar sein, also beispielsweise auf der Eingangsseite der Website positioniert oder zumindest auf dieser verlinkt sein. In der Erklärung ist über die Verfahrensweise bei der Verarbeitung personenbezogener Daten, die bei der Bereitstellung und Nutzung der jeweiligen Verwaltungsdienstleistung im Internet anfallen, zu informieren. Zu unterrichten ist dabei u.a. auch über die Speicherung von Daten in Logfiles und über die Verwendung und Funktionsweise von Cookies. Dies hat auf eine leicht verständliche Art und Weise zu geschehen. Außerdem empfiehlt es sich, den jeweiligen Datenschutzbeauftragten als Ansprechpartner für Datenschutzfragen zu benennen und seinen Namen und seine Kontaktdaten in der Datenschutzerklärung aufzuführen.

Obwohl die eben skizzierten gesetzlichen Vorgaben des Telemediengesetzes bzw. der Vorgängervorschriften im Teledienstedatenschutzgesetz und im Mediendienste-Staatsvertrag bereits seit beinahe zehn Jahren geltendes Recht darstellen, kommt es in der Praxis auch gegenwärtig noch vor, dass Behörden die Pflicht zur Anbieterkennzeichnung und/oder zur Bereitstellung einer Datenschutzerklärung auf ihrer Website nicht erfüllen.[229] Natürlich gibt es aber auch E-Government-Websites, die den gesetzlichen Anforderungen in vollem Umfang genügen – als Beispiel für eine Datenschutzerklärung, die in gut verständlicher Art und Weise über viele Details der Erhebung und Verwendung

[225] Zu den (sicheren) elektronischen Zahlungssystemen vgl. bereits die Abschnitte 3.3.2 und 4.9.2 in dieser Arbeit. Außerdem siehe etwa [Neumann 2003]. Ein Überblick über Zahlungsmethoden im Bereich des E-Government findet sich im Kapitel „Sichere Zahlungsverfahren für E-Government“ des Bundesamts für Sicherheit in der Informationstechnik (BSI), abrufbar unter http://www.bsi.bund.de/fachthem/egov/download/4_Zahlv.pdf (letzter Zugriff im Oktober 2007).

[226] Nach dieser Vorschrift sind Anbieter von Telemedien auch zur Unterrichtung über die Verarbeitung personenbezogener Daten in sog. Drittstaaten verpflichtet. Dies spielt aber im Rahmen des E-Government typischerweise keine Rolle. Im Übrigen entfällt die Unterrichtungspflicht dann, wenn eine Unterrichtung bereits anderweitig erfolgt ist.

[227] Synonym werden insoweit auch die Begriffe Datenschutzhinweis, Datenschutz-Policy oder Privacy Policy verwendet.

[228] Einzelheiten hierzu finden sich in den Handlungsempfehlungen „Datenschutzgerechtes eGovernment“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, S. 35 ff., abrufbar unter http://cdl.niedersachsen.de/blob/images/C1358174_L20.pdf (letzter Zugriff im Oktober 2007).

[229] 22. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz vom 29. Januar 2007, Textziffer 3.17, S. 20, abrufbar unter http://www.datenschutz-bayern.de/tbs/tb22/tb22.pdf (letzter Zugriff im Oktober 2007). Auf einigen behördlichen Websites stellt die Datenschutzerklärung einen Bestandteil der Rubrik Impressum dar. Insoweit ist anzumerken, dass es im Hinblick auf eine möglichst einfache Auffindbarkeit vorzugswürdig ist, auf der Website für die Datenschutzerklärung eine eigene Rubrik mit einem eindeutigen Titel einzurichten.

personenbezogener Daten informiert, sei an dieser Stelle die „Datenschutzerklärung für Internetangebote der Stadt Nürnberg“[230] genannt.

3.2.5.4 Fazit

Je mehr Verwaltungsdienstleistungen im Rahmen von E-Government zur Verfügung gestellt und je stärker diese von den Bürgern nachgefragt werden, umso mehr digitale Teilidentitäten und diesen zugeordnete Daten fallen in diesem Zusammenhang an. Technisch gesehen ermöglicht dies umfangreiche Verkettungen etwa anhand von Cookies, Zertifikatsinformationen, staatlichen Identifikationsnummern oder Informationen wie Name und Geburtsdatum. Da die Offenlegung der Identität des Bürgers in vielen E-Government-Anwendungen vorausgesetzt wird, kann der Einzelne dieser Situation regelmäßig nicht durch ein anonymes oder pseudonymes Auftreten gegenüber der Verwaltung begegnen. Umso wichtiger ist es, dass durch verständliche und leicht auffindbare Datenschutzerklärungen ein Höchstmaß an Transparenz für den Bürger geschaffen wird. Diesen Anforderungen genügen manche der in der Praxis verwendeten Websites allerdings noch nicht. Ein sinnvolles Instrument zur Verhinderung von Verkettungen anhand von staatlichen Identifikationsnummern stellt das österreichische Bürgerkartenkonzept mit seinen bereichsspezifischen Personenkennzeichen dar.

3.2.6 E-Participation

3.2.6.1 Einleitung

Die Bezeichnung E-Participation setzt sich aus den beiden Begriffen „electronic“ (engl. für elektronisch, rechnergestützt) und „Participation“ (engl. für Beteiligung, Teilnahme) zusammen. Bei E-Participation handelt es sich um eine spezielle Ausprägung des E-Government – genauer gesagt ist E-Participation eine Erscheinungsform der sog. E-Democracy.

Wie bereits ausgeführt, lässt sich der Begriff E-Government in die Bereiche E-Administration, E-Democracy und E-Justice untergliedern.[231] Charakteristisch für E-Democracy ist der Einsatz von IuK-Technologien zwecks elektronischer Abbildung bzw. Weiterentwicklung demokratischer Prozesse. Nach der bereits vorgestellten Speyerer Definition von E-Government ist hierunter insbesondere der „Einsatz moderner Informations- und Kommunikationstechnologien für Bürgerinitiativen, Parteien, Politiker, Wahlkämpfe bis hin zur Durchführung von Wahlen und Volksabstimmungen“ zu verstehen.[232]

Üblicherweise wird bei E-Democracy zwischen den beiden Bereichen E-Voting und E-Participation unterschieden.[233] Der Begriff E-Voting bezeichnet elektronische Wahlen und Abstimmungen, die etwa als Online-Wahlen oder mittels elektronischer Wahlmaschinen durchgeführt werden. Er zielt damit auf einen Akt der Entscheidung ab. Bei E-Participation geht es hingegen um den Prozess der Willensbildung und Entscheidungsfindung. Umfasst werden also alle via IuK-Technologien zur Verfügung gestellten Verfahren einer Beteiligung von Bürgern am politischen Willensbildungsprozess. Auch wenn sie in engem Zusammenhang zu einer späteren Abstimmung stehen, sollen (elektronische) Verfahren, die eine solche lediglich vorbereiten bzw. Voraussetzung für diese sind, vorliegend nicht dem E-Voting, sondern der E-Participation zugerechnet werden.[234]

Bei der E-Participation geht es nicht (nur) um eine bloße Digitalisierung bereits vorhandener Verfahren, sondern auch um die Entwicklung und Etablierung neuer Beteiligungsmöglichkeiten für die Bürger. Einen ersten Schritt in diese Richtung stellen beispielsweise politische Diskussionsforen oder

[230] http://www.nuernberg.de/internet/portal/generisch/datenschutz.html (letzter Zugriff im Oktober 2007).
[231] Vgl. bereits oben im Abschnitt 3.2.5.
[232] Speyerer Definition S. 5, abrufbar unter http://foev.dhv-speyer.de/ruvii/Sp-EGov.pdf (letzter Zugriff im Oktober 2007).
[233] Vgl. etwa [Märker 2005, S. 95]. Einzelheiten zur Terminologie finden sich in der [E-Participation-Studie 2006, S. 5 ff.], abrufbar unter http://www.britishcouncil.de/pdf/e_participationdt.pdf (letzter Zugriff im Oktober 2007).
[234] So ist dann beispielsweise das Volksbegehren der E-Participation, der Volksentscheid selbst hingegen dem E-Voting zuzuordnen.

Chats im Internet dar.[235] Als weitergehende Möglichkeiten kommen die Einrichtung virtueller Räume für Besprechungen zwischen Verwaltung und Bürgerinitiativen bzw. Interessenverbänden oder die elektronische Organisation verschiedener direktdemokratischer Elemente wie Volksbegehren oder Bürgerbegehren in Betracht.[236]

3.2.6.2 Teilhaberechte und elektronische Partizipation

Bürger der Bundesrepublik Deutschland können auf vielfältige Art und Weise am politischen Leben teilhaben.[237] Dies können sie zum einen durch Beteiligung an Wahlen und Abstimmungen tun, zum anderen steht ihnen eine Vielzahl weiterer Möglichkeiten zur Teilhabe am politischen Leben zur Verfügung, deren Ausübung mittels IuK-Technologien dem Bereich der E-Participation zuzuordnen ist bzw. – sofern noch kein entsprechendes Angebot besteht – diesem Bereich zuzuordnen wäre. Exemplarisch werden an dieser Stelle nur Volksbegehren und Bürgerbegehren, das Petitionsrecht sowie die Beteiligung der Öffentlichkeit im Bauplanungsrecht vorgestellt.

3.2.6.2.1 Volksbegehren und Bürgerbegehren

Anders als auf Bundesebene, wo das Grundgesetz einen Volksentscheid nur für Maßnahmen zur Neugliederung des Bundesgebiets vorsieht, besteht mittlerweile für die Bürger auf Landes- und kommunaler Ebene die Möglichkeit, Abstimmungen über unterschiedliche Sachthemen herbeizuführen. Voraussetzung für die eigentliche Abstimmung, die auf Landesebene als Volks- und auf kommunaler Ebene als Bürgerentscheid bezeichnet wird, ist dabei stets die vorherige (erfolgreiche) Durchführung eines so genannten Volks- bzw. Bürgerbegehrens. Die Bürger bekunden im Rahmen eines solches Begehrens mittels einer Sammlung von Unterschriften ihren Willen, dass zu einer bestimmten Sachfrage ein Volks- bzw. Bürgerentscheid durchgeführt wird.

Die gesetzlichen Grundlagen für Volksbegehren finden sich in den Landesverfassungen der einzelnen Bundesländer sowie in den jeweiligen Volksabstimmungsgesetzen.[238] Die rechtlichen Voraussetzungen für die Durchführung von Bürgerbegehren sind hingegen in erster Linie in den Gemeinde- und Landkreisordnungen der Bundesländer geregelt.[239] Nach den einschlägigen Bestimmungen können bislang weder Volks- noch Bürgerbegehren elektronisch durchgeführt werden.[240]

3.2.6.2.2 Petitionsrecht

Das Petitionsrecht ist als Grundrecht in Art. 17 GG und in ähnlichen Bestimmungen verschiedener Landesverfassungen festgeschrieben. Es räumt jedem Menschen das Recht ein, sich einzeln oder in Gemeinschaft mit anderen mit Bitten oder Beschwerden an die jeweils zuständigen Stellen oder die Volksvertretung zu wenden. Darüber hinaus hat derjenige, der eine zulässige Petition einreicht, auch einen subjektiv-rechtlichen Anspruch darauf, dass die angegangene Stelle seine Eingabe nicht nur entgegennimmt, sondern sie auch sachlich prüft und ihm zumindest die Art der Erledigung schriftlich mitteilt.[241]

Art. 17 GG bestimmt, dass Eingaben schriftlich einzureichen sind. Dieses Gebot der Schriftlichkeit wird allerdings nach der hier vertretenen Ansicht auch bei einer Einreichung per Fernschreiben, Tele-

[235] So etwa [Märker/Trénel 2003, S. 18].
[236] Vgl. [Schuppan/Reichard 2002, S. 106].
[237] Eine gute Übersicht über die verschiedenen Arten der politischen Teilhabe findet sich beispielsweise unter http://www.buergergesellschaft.de/politische-teilhabe/ (letzter Zugriff im Oktober 2007).
[238] Vgl. etwa Art. 42 der Verfassung des Landes Schleswig-Holstein und das schleswig-holsteinische Gesetz über Initiativen aus dem Volk, Volksbegehren und Volksentscheid (VAbstG SH).
[239] Insoweit vgl. etwa § 16g der Gemeindeordnung für Schleswig-Holstein (GO SH) und § 16f der Kreisordnung für Schleswig-Holstein (KrO SH).
[240] So verlangen beispielsweise § 15 S. 1 VAbstG SH (für das Volksbegehren) sowie § 7 Abs. 4 S. 1 der Landesverordnung zur Durchführung der GO SH und § 5 Abs. 4 S. 1 der Landesverordnung zur Durchführung der KrO SH (für das Bürgerbegehren) die persönliche und handschriftliche Unterschrift des Bürgers und schließen damit die Durchführung eines elektronischen Verfahrens aus.
[241] BVerfGE 2, 225 (230) = NJW 1953, 817.

gramm, Telefax, E-Mail oder via Online-Formular im Internet gewahrt[242], weshalb eine Petition also auch auf elektronischem Wege eingereicht werden kann (sog. Online- oder E-Petition). Folgerichtig bietet der Deutsche Bundestag interessierten Personen im Rahmen des Projekts E-Petition seit September 2005 die Möglichkeit der Initiierung oder Unterstützung einer Online-Petition an.[243] Konkret können sog. öffentliche Petitionen initiiert und während eines bestimmten Zeitraums auch von weiteren Personen durch Hinzufügen ihres Namens unterstützt werden.[244] Darüber hinaus besteht auch die Möglichkeit, sich an Online-Diskussionen zu den einzelnen Petitionen zu beteiligen. Das Online-Petitionssystem basiert auf einem bereits früher implementierten System des Schottischen Parlaments, weshalb der Server für die Öffentlichen Petitionen gegenwärtig vom International Teledemocracy Centre an der Napier Universität in Edinburgh betrieben wird.[245]

3.2.6.2.3 Beteiligung der Öffentlichkeit an der Bauleitplanung

Die Aufgabe der Bauleitplanung besteht darin, die bauliche und sonstige Nutzung der Grundstücke in einer Gemeinde vorzubereiten und zu leiten. Die Gemeinden haben Bauleitpläne aufzustellen, sobald und soweit dies für die städtebauliche Entwicklung und Ordnung erforderlich ist. Insoweit ist zwischen vorbereitenden Bauleitplänen (sog. Flächennutzungsplänen) und verbindlichen Bauleitplänen (sog. Bebauungsplänen) zu unterscheiden. Nach § 3 des Baugesetzbuches (BauGB) ist die Öffentlichkeit an der Bauleitplanung zu beteiligen. Bereits zu Beginn eines Planungsverfahrens sind die Bürger über die allgemeinen Ziele und Zwecke der Planung, über unterschiedliche Lösungsmöglichkeiten sowie über die voraussichtlichen Auswirkungen zu unterrichten. Außerdem muss ihnen auch Gelegenheit zur Äußerung und Erörterung gegeben werden. Liegt dann ein konkreter Entwurf eines Bauleitplans vor, so schließt sich die zweite Stufe der Öffentlichkeitsbeteiligung an: Jeder Entwurf ist zusammen mit einem Erläuterungsbericht bzw. einer Begründung für die Dauer von mindestens einem Monat öffentlich auszulegen, wobei Ort und Dauer der Auslegung spätestens eine Woche zuvor bekannt gemacht werden müssen. Die Auslegung muss dergestalt erfolgen, dass jeder an der Planung Interessierte ohne weiteres Einblick in die Unterlagen nehmen kann. Während der Dauer der Auslegung können von jedermann – also nicht nur von Betroffenen und Beteiligten – Stellungnahmen zu dem jeweiligen Bauleitplanentwurf abgegeben werden. Die Gemeindeverwaltung muss zulässige Stellungnahmen prüfen und den Einsendern das Ergebnis mitteilen.

Der im Jahre 2004 in das Baugesetzbuch eingefügte § 4a Abs. 4 stellt ausdrücklich klar, dass bei der Öffentlichkeitsbeteiligung ergänzend elektronische Informationstechnologien genutzt werden können.[246] Beispiele für eine solche Nutzung sind die Einstellung des Entwurfs des jeweiligen Bauleitplans in das Internet oder die Abgabe von Stellungnahmen der Bürger via E-Mail oder mittels eines Online-Formulars. Eine Verpflichtung zur IT-Nutzung besteht für die Gemeindeverwaltung bislang hingegen nicht.

---

[242] So grundsätzlich auch Krüger/Pagenkopf in [Sachs 2003, Art. 17 Rn. 9]. Vgl. auch [Krings 2004, S. 476]. Ausführlich mit der Frage nach der Zulässigkeit der Einlegung einer Petition via E-Mail befasst sich [Schmitz 2003].

[243] Nach Ziffer 4 Abs. 1 Satz 3 der Grundsätze des Petitionsausschusses über die Behandlung von Bitten und Beschwerden (Verfahrensgrundsätze) ist die Schriftlichkeit bei elektronisch übermittelten Petitionen dann gewahrt, wenn der Urheber und dessen Postanschrift ersichtlich sind und das im Internet für elektronische Petitionen zur Verfügung gestellte Formular verwendet wird. Allerdings gibt es Stimmen in der rechtswissenschaftlichen Literatur, die die Vereinbarkeit dieser Lösung mit dem Schriftformerfordernis des Art. 17 GG verneinen (so etwa [Kellner 2007]).

[244] Die Petitionen werden auf der Website des Projekts E-Petition unter http://itc.napier.ac.uk/e-Petition/bundestag/ (letzter Zugriff im Oktober 2007) veröffentlicht.

[245] Aus Datenschutzsicht ist dieser Umstand kritisch zu bewerten, weil nicht ersichtlich ist, warum der Dienst nicht auch auf dem „regulären“ Server des Deutschen Bundestages (http://www.bundestag.de/ (letzter Zugriff im Oktober 2007)) angeboten werden können sollte.

[246] Die Vorschrift soll zur ergänzenden Nutzung elektronischer Informationstechnologie anregen, um das Maß an Transparenz der Beteiligungsverfahren für Öffentlichkeit und Behörden zu erhöhen. § 4a ist durch das Europarechtsanpassungsgesetz (EAG) Bau im Jahre 2004 in das Baugesetzbuch eingefügt worden.

3.2.6.3 Status Quo von E-Participation in Deutschland

Wie bereits die soeben vorgestellten Beteiligungsverfahren deutlich gemacht haben, gibt es in Deutschland für die Bürger mittlerweile erste Möglichkeiten einer elektronischen Beteiligung am politischen Leben.[247] Überwiegend handelt es sich hierbei um digitale Varianten bereits existenter Partizipationsmöglichkeiten, d.h., die jeweils für eine politische Teilhabe erforderlichen Informationen werden online zur Verfügung gestellt und der Bürger erhält die Möglichkeit, seinen Beitrag auf elektronischem Wege an die Verwaltung zu übermitteln. Wie etwa das Beispiel von Bürger- und Volksbegehren zeigt, ist Letzteres für den politisch interessierten Bürger allerdings in vielen Fällen aufgrund restriktiver gesetzlicher Vorgaben (noch) nicht möglich. Insgesamt ist festzustellen, dass die Verwaltung bislang noch nicht gesetzlich dazu verpflichtet ist, Verfahren zur elektronischen Partizipation anzubieten. Das Projekt E-Petition des Deutschen Bundestages zeigt allerdings zumindest ansatzweise, welche neuen Gestaltungsmöglichkeiten den Bürgern im Rahmen von E-Participation zur Verfügung gestellt werden können: Konkret wird es hier einem Petenten ermöglicht, via Internet Gleichgesinnte zu finden, die sich seinem Anliegen anschließen. Zudem besteht für alle interessierten Bürger die Möglichkeit, online über eine bestimmte Petition zu diskutieren.

3.2.6.4 E-Participation und Verkettung

Wie bereits erwähnt, stellt E-Participation einen Unterfall des E-Government dar. Deshalb sind hier hinsichtlich der Thematik einer Verkettung digitaler Identitäten grundsätzlich die bereits im Abschnitt 3.2.5 zu E-Government genannten Aspekte zu berücksichtigen. Betrachtet man die gesetzlichen Vorgaben für die verschiedenen Arten politischer Partizipation bzw. die entsprechende Verwaltungspraxis, so wird schnell deutlich, dass auch hier vom Bürger vielfach die Offenlegung seiner Identität verlangt wird.

Dies gilt etwa für die oben vorgestellte Möglichkeit einer Teilnahme an Volks- bzw. Bürgerbegehren. Wer sich an einem solchen beteiligen will, kann sich in Eintragungslisten oder Einzelanträge eintragen. Anzugeben sind hierbei der Familienname, der Vorname, der Tag der Geburt, der Wohnort mit Postleitzahl, Straße und Hausnummer sowie das Datum der Unterzeichnung.[248] Wie bereits erwähnt, ist der Eintrag sodann persönlich und handschriftlich zu unterzeichnen.

Im Anschluss hieran überprüft die zuständige (Melde-)Behörde alle Antragslisten und Einzelanträge auf Richtigkeit der Eintragungen und Berechtigung der Unterzeichner zur Teilnahme an dem Volks- bzw. Bürgerbegehren hin und stellt sodann die Anzahl der gültigen und ungültigen Eintragungen fest. Werden Eintragungslisten verwendet, können die im Rahmen der Eintragung angegebenen Daten im Übrigen nicht nur von den zuständigen Behörden, sondern auch von (späteren) Mitunterzeichnern eingesehen werden.

Auch wenn dies gegenwärtig aufgrund der gesetzlichen Vorgaben noch nicht möglich ist, erscheint es doch durchaus als möglich, dass zukünftig die Voraussetzungen für eine elektronische Durchführung von Bürger- und Volksbegehren geschaffen werden. Da eine solche elektronische Variante wesentlich schneller und leichter organisiert werden könnte als die bislang verwendete herkömmliche Methode, würde den Bürgern diese konkrete Art der politischen Teilhabe hierdurch deutlich erleichtert werden. Im Zuge der Ermöglichung einer solchen elektronischen Variante sollte dann allerdings auch darüber nachgedacht werden, ob eine Offenlegung der Identität der Bürger zur Durchführung eines solchen Volks- oder Bürgerbegehrens tatsächlich erforderlich ist oder ob nicht auch auf anderem Wege

[247] Insoweit sei noch darauf hingewiesen, dass die beiden gemeinnützigen Organisationen BritishCouncil und pol-di.net via Internet recht umfassende Informationen zum aktuellen Status Quo von E-Participation in Deutschland und Großbritannien zur Verfügung stellen. So bieten die beiden genannten Organisationen unter http://www.britishcouncil.de/pdf/e_participationdt.pdf die [E-Participation-Studie 2006] zum Abruf an (letzter Zugriff im Oktober 2007), außerdem wird unter http://www.e-participation.net/ (letzter Zugriff im Oktober 2007) der Versuch unternommen, möglichst viele internetbasierte Partizipationsprojekte in Deutschland und Großbritannien aufzulisten, mit einer kurzen Inhaltsangabe zu versehen und zu verlinken.

[248] Vgl. etwa für Schleswig-Holstein § 6 Abs. 1 Nr. 3 + 5 der Landesverordnung zur Durchführung des VabstG (für das Volksbegehren) sowie § 7 Abs. 4 der Landesverordnung zur Durchführung der GO (für das Bürgerbegehren) und § 5 Abs. 4 S. 1 1. HS. der Landesverordnung zur Durchführung der KrO (für das Volksbegehren).

(beispielsweise durch Verwendung pseudonymer digitaler Signaturen nebst bestätigten Attributen) sichergestellt werden kann, dass jede partizipierende Person auch nur einmal eine Unterschrift leistet und dass nur hierzu berechtigte Personen[249] an dem jeweiligen Begehren teilnehmen können.

Entsprechendes gilt auch für die Abgabe von Petitionen, die nach allgemeiner Auffassung nicht anonym eingereicht werden dürfen.[250] Dies erscheint nicht zuletzt deshalb als problematisch, weil beispielsweise das Aufzeigen bestimmter Missstände durchaus auch dann sinnvoll sein kann, wenn es anonym erfolgt. Auch kann der Petent in solchen Fällen aus vielen Gründen ein Interesse daran haben, lediglich anonym in Erscheinung zu treten. Wäre ein anonymes Auftreten zulässig, so würde hierdurch implizit auch ein Verzicht auf eine schriftliche Mitteilung der angegangenen Behörde erklärt werden. Im Übrigen sehen etwa die Richtlinien für die Behandlung von öffentlichen Petitionen im Rahmen des Projekts E-Petition des Bundestages vor, dass sowohl der Hauptpetent als auch eventuelle Mitunterzeichner einer Petition neben ihrem Namen auch ihre Wohn- und ihre E-Mail-Adresse angeben müssen – online veröffentlicht werden dann Name und Adresse des Hauptpetenten sowie der Name des Mitunterzeichners und das Bundesland, in dem er gegenwärtig wohnt. Schließlich wird auch bei Stellungnahmen im Rahmen der Beteiligung der Öffentlichkeit in der Bauleitplanung verlangt, dass der die Stellungnahme Abgebende seinen Namen und seine Adresse angibt.

3.2.6.5 Fazit

Gegenwärtig gibt es in Deutschland verschiedene Möglichkeiten einer elektronischen Partizipation am politischen Leben, bei denen es sich überwiegend um digitale Varianten bereits existenter Beteiligungsrechte handelt. Eine Herausforderung bestünde darin, neue Angebote zu entwickeln und zur Verfügung zu stellen, die den Bürgern zuvor noch nicht vorhandene Chancen zur politischen Partizipation bieten. Nachzudenken wäre in diesem Zusammenhang darüber, ob nicht die gesetzlichen Regelungen bei einigen Varianten der politischen Beteiligung der Bürger dahingehend geändert werden sollten, dass die Offenlegung der Identität der Bürger nicht mehr unbedingt erforderlich ist. Insofern könnte in einigen Konstellationen (z.B. hinsichtlich der Einlegung von Online-Petitionen) in Erwägung gezogen werden, auch ein anonymes Auftreten des Bürgers zu gestatten – in anderen Konstellationen (z.B. bei Volks- und Bürgerbegehren) sollte darüber nachgedacht werden, ob es dort nicht ausreicht, unter Verwendung von Pseudonymen festzustellen, ob eine Person zum zur Partizipation berechtigten Personenkreis gehört und auch tatsächlich nur eine Unterschrift geleistet hat.

3.2.7 Strafverfolgung und Gefahrenabwehr

3.2.7.1 Einleitung

Man kann grundsätzlich die polizeilichen Aufgabenbereiche präventive Gefahrenabwehr und repressive Strafverfolgung unterschieden. Beim Tätigwerden der Polizei werden regelmäßig personenbezogene Daten erhoben, verarbeitet, übermittelt und abgeglichen. Denn als Täter einer Straftat oder als Störer im Sinne des Polizeirechts stehen natürliche Personen im Zentrum der Ermittlungen und Gefahrenprognosen der Polizei.[251] Nachstehend soll ein Überblick über polizeiliche Befugnisse ohne Anspruch auf Vollständigkeit gegeben werden.[252]

Die Polizei wird im Rahmen der Gefahrenabwehr tätig, wenn sie vorbeugend zur Verhütung einer Rechtsgutsverletzung handelt. Dabei wurde lange angeknüpft an das Vorliegen einer Gefahr, dem Bevorstehen eines schädigenden Ereignisses. Eine Gefahr[253] liegt danach vor, wenn ein Rechtsgut auf Grund konkreter tatsächlicher Anhaltspunkte und zeitlich nah gefährdet ist. Geregelt sind die Kompe-

[249] Also solche, die Einwohner der jeweiligen Kommune sind oder in dem entsprechenden Bundesland wohnen.
[250] [Krings 2004, S. 476].
[251] Ausführlich zur Informationsverarbeitung im Polizei- und Strafverfahrensrecht [Petri 2007].
[252] Die Landespolizeigesetze enthalten eine Vielzahl von unterschiedlichen Eingriffsschwellen für verschiedene Befugnisse.
[253] Zum Gefahrenbegriff im Polizeirecht: [Poscher 2001]. Zur Abgrenzung zwischen Gefahrenabwehrrecht und Verdachtsschöpfungsermittlungen: [Keller 1990].

tenzen und Pflichten der Polizei im Rahmen der Gefahrenabwehr in erster Linie in den Polizeigesetzen der Länder. Auf Bundesebene sind zudem das BKA-Gesetz, das Zollfahndungsdienstgesetz (ZfdG) und das Bundespolizeigesetz von Bedeutung. Die Polizeigesetze der Länder enthalten auch Kompetenzen im Gefahrenvorfeld, also der Verhütung von nicht unmittelbar bevorstehenden Rechtsgutsverletzungen. Die polizeilichen Eingriffsbefugnisse sind in den zurückliegenden Jahren und Jahrzehnten immer weiter vorverlagert worden[254] bis hin zu Verdachtsgewinnungseingriffen weit im Vorfeld eines konkreten Verdachts.[255] Da es bei solchen Maßnahmen nicht darum geht, gegen konkrete Störer vorzugehen, sondern „riskante“ Personen oder Ereignisse erst aufgespürt werden sollen, knüpfen Verdachtsgewinnungseingriffe nicht an das Bestehen einer Gefahr oder Störereigenschaft an, sondern sind teilweise sogar anlasslos möglich. Zudem wenden sie sich oft gegen einen großen Personenkreis, da ein potenzieller Täter erst aufgefunden werden soll.

Als Strafverfolgung bezeichnet man das Handeln der Polizei und Staatsanwaltschaft, das auf die Vergangenheit gerichtet ist und dazu dient, Straftaten aufzuklären und den Täter einer Bestrafung zuzuführen. Die rechtlichen Grundlagen der polizeilichen Aufgaben und Kompetenzen im Rahmen der Strafverfolgung finden sich insbesondere in der Strafprozessordnung (StPO) und im Strafgesetzbuch (StGB).

Nachstehend wird ein Überblick gegeben über die Ermittlungsmethoden, die der Polizei zur Verfügung stehen. Im Rahmen all dieser Ermittlungsbefugnisse können personenbezogene Daten erhoben und verarbeitet werden. Die Polizeigesetze, die Strafprozessordnung und weitere in Frage kommende Gesetze enthalten insoweit bereichsspezifische Datenschutzregelungen.

3.2.7.2 Gefahrenabwehr

Polizeiliche Datenverarbeitung bedarf grundsätzlich einer bereichsspezifischen, präzisen gesetzlichen Grundlage.

Die Befugnis zum polizeilichen Tätigwerden ist im Rahmen der Gefahrenabwehr über die polizeigesetzlichen Generalklauseln abgebildet. Bei grundrechtsintensiven Datenerhebungen finden sich zudem spezielle Befugnisnormen in den Polizeigesetzen.

Die Polizeigesetze sehen dabei eigene Klauseln über die Datenerhebung[256], Datenübermittlung und Speicherung von Daten vor.

Eine Übersicht der speziellen Datenerhebungsbefugnisse gibt Tabelle 11:

[254] Vgl. dazu [Hoffmann-Riem 2002].

[255] So vgl. z.B. bei der Rasterfahndung BVerfG, Beschluss vom 04.04.2006 – 1 BvR 518/02 = NJW 2006, 1939, abrufbar unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20060404_1bvr051802.html (Pressemitteilung unter http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg06-040.html; letzter Zugriff jeweils im Oktober 2007) oder bei Polizeikontrollen ohne Gefahrverdacht [Möllers 2000].

[256] In Schleswig-Holstein: Datenerhebungsgeneralklausel § 179 LvwG SH, spezielle Datenerhebungsklauseln §§ 180 ff. LvwG SH, Datenspeicherung §§ 188-190 LvwG SH, Datenübermittlungsklausel §§ 191-195a LvwG SH.

	Rechtsgrundlage	Bild	Gesprochenes Wort	Biometrische Daten	Standortdaten	Telekomm.-daten	Sonstige
Generalklausel	§ 179 LVwG SH						X
Kennzeichenscanning	§ 184 Abs. 5 LVwG SH				X		X
Schleierfahndung	§ 180 Abs. 3 LVwG SH						X
Video- und Tonüberwachung des öffentlichen Raumes	§ 184 Abs. 2 LVwG SH	X	X				
Erkennungsdienstliche Maßnahmen	§ 183a LVwG SH	X	X	X			
DNA	§ 183a LVwG SH			X			
Telekommunikationsüberwachung	§ 185a LVwG SH		X		X	X	

Tabelle 11: Bereichsspezifische Vorschriften des Polizeirechts

Die Datenspeicherung, also das Erfassen, Aufnehmen oder Aufbewahren von Daten zum Zweck einer weiteren Verwendung findet durch die Polizei sowohl in elektronischer Form als auch in Akten statt. Konventionelle Akten werden teilweise durch Einscannen elektronisch erfasst oder auch nur indiziert. Durch eine Automatisierung können neue und erleichterte Zugriffs- und Nutzungsmöglichkeiten entstehen. Insbesondere die elektronische Datenspeicherung bietet die Möglichkeit, über einen Betroffenen erfasste Informationen in verschiedenen Zusammenhängen neu zu verwenden.[257] Bei jeder Speicherung von Daten ist die Erforderlichkeit des damit verbundenen Eingriffs neu zu prüfen. Eine Speicherung personenbezogener Daten durch die Polizei darf grundsätzlich erfolgen, wenn dies zur Erfüllung polizeilicher Aufgaben erforderlich ist. Die Speicherung darf für die Zwecke stattfinden[258], für die Informationen erhoben wurden. Eine zweckändernde Verwendung ist durch die Polizeigesetze in weitem Umfang zugelassen.

Eine Übermittlung von Daten liegt vor, wenn gespeicherte oder durch Datenverarbeitung gewonnene Daten an einen Dritten bekannt gegeben werden. Einige Polizeigesetze der Länder enthalten Bedingungen für die Befugnis zur Datenübermittlung. Grundsätzlich gilt, dass personenbezogene Daten nur zu dem Zweck übermittelt werden dürfen, zu dem die Informationen erlangt oder gespeichert wurden. Das Zweckbindungsprinzip wird auch bei der Übermittlung personenbezogener Daten im Polizei- und Strafverfahrensrecht vielfach durchbrochen. In den zurückliegenden Jahren wurde das Zweckbindungsprinzip aufgeweicht. Wenn weitere Rechtsvorschriften eine Informationsübermittlung vorsehen, tritt nämlich der Grundsatz der Zweckbindung zurück. Eine Datenübermittlung kann dabei an ausländische Polizeibehörden oder zwischenstaatliche Einrichtungen vorgesehen sein. Auch an andere öffentliche Stellen, die im Rahmen der Gefahrenabwehr tätig sind, kann eine Übermittlung gestattet sein. Schließlich lassen einige Polizeigesetze eine Datenübermittlung an nichtöffentliche Stellen unter konkreten Bedingungen zu, zum Beispiel für eine Öffentlichkeitsfahndung.

Vielfach wird Datenübermittlung durch automatische Abrufverfahren ermöglicht. Dabei richten Datenübermittler und Datenempfänger ein automatisiertes Verfahren ein, das einen Abruf personenbezogener Daten beim Datenübermittler erlaubt. Solche Verfahren werden eingesetzt bei Online-Abrufen aus den Melderegistern, dem Ausländerzentralregister, INPOL oder dem Zentralen Verkehrs-

[257] [Petri 2007, S. 938 Rn. 352].
[258] Kritisch zur weitgehenden Aushebelung des Zweckbindungsgrundsatzes [Petri 2007, S. 939 Rn. 355 ff.].

informationssystem (ZEVIS) des Kraftfahrzeugbundesamtes. Dabei werden im Verfahren INPOL zur vorbeugenden Bekämpfung von Straftaten massenhaft Daten[259] zweckungebunden gespeichert und sind bundesweit abrufbar.

Schließlich verfügt die Polizei über Befugnisse zum Abgleich von personenbezogenen Daten mit eigenen Datenbeständen. Dabei soll überprüft werden, ob ein Gegenstand (Fahrzeug) oder eine Person bereits polizeilich erfasst ist. Dazu kann ein Abgleich zum Beispiel mit beim Bundeskriminalamt geführten Personenfahndungsdateien oder Sachfahndungsdateien stattfinden. Ein weiterer Anwendungsfall des Datenabgleichs ist die Rasterfahndung.

3.2.7.3 Strafverfolgung

Zur Informationsgewinnung und Ermittlung im Rahmen der Strafverfolgung kann sich die Polizei eigener Mittel bedienen. Zusätzlich ist sie auf Angaben angewiesen, die Dritte erhoben haben. Dabei erfolgt der Zugriff nicht nur auf Daten von Beschuldigten, sondern kann sich auch gegen Dritte richten. Eine Übermittlung von personenbezogenen Daten, die Unternehmen, Behörden oder natürlichen Personen erhoben haben, kann ebenso Gegenstand polizeilicher Datenverarbeitung sein. Die Polizei kann Auskunftsersuchen an Unternehmen, Behörden und natürliche Personen stellen, §§ 161, 163 StPO.

Behörden sind gegenüber der Staatsanwaltschaft oder den für sie tätig werdenden Beamten des Polizeidienstes grundsätzlich nach §§ 161, 163 StPO zur Auskunft verpflichtet. Es gilt § 15 Abs. 1 i.V.m. 14 Abs. 2 BDSG für die Weitergabe von Daten an die Staatsanwaltschaft oder Polizei.[260] Behörden haben also bei einer Anfrage der Staatsanwaltschaft die Schlüssigkeit des Auskunftsersuchens zu prüfen und die Staatsanwaltschaft muss ein rechtliches Interesse an der Kenntnis der angefragten Daten glaubhaft machen. Die Ermittlungsgeneralklausel der §§ 161, 163 StPO stellt allerdings eine Ermächtigungsgrundlage nur für weniger intensive Grundrechtseingriffe dar.[261] Grundrechtsintensivere Maßnahmen, wie beispielsweise Eingriffe in das das Steuergeheimnis[262] oder das Sozialgeheimnis[263], bedürfen einer ausdrücklichen Ermächtigungsgrundlage oder einer informierten Einwilligung des Betroffenen.

An Unternehmen oder Personen kann die Staatsanwaltschaft oder die Polizei ebenfalls ein Auskunftsersuchen stellen. Wenn Unternehmen oder natürliche Personen nicht bereit sind, die gewünschte Auskunft zu geben, kann entweder die förmliche Vernehmung erzwungen[264] werden, die Herausgabe[265] verlangt oder die Durchsuchung[266] oder Beschlagnahme[267] angeordnet werden. Eingeschränkte Auskunftspflichten bestehen beispielsweise für Banken.

Sowohl für Behördenmitarbeiter, als auch für Mitarbeiter von Unternehmen und anderen Personen kann ein Zeugnisverweigerungsrecht[268] bestehen. Eine Aussage- oder Übermittlungspflicht entfällt dann für die berechtigte Person.

Im Rahmen der Strafverfolgung verfügt die Polizei über zahlreiche speziell normierte Ermittlungsmethoden, bei denen personenbezogene Daten erhoben und verarbeitet werden. Eine Übersicht dieser Methoden, der Rechtsgrundlage und der dabei üblicherweise anfallenden Daten folgt nachstehend beispielhaft in Tabelle 12:

[259] Vgl. z.B. § 189 Abs. 1 S. 2 LVwG SH.
[260] [Meyer-Goßner 2005, § 161 Rn. 1a].
[261] Vgl. [Warg 2006].
[262] Geregelt in § 30 Abgabenordnung.
[263] Geregelt in § 35 Sozialgesetzbuch I.
[264] Vgl. §§ 161a, 51 StPO.
[265] Vgl. § 95 StPO.
[266] Vgl. § 103 StPO.
[267] Vgl. §§ 94 ff. StPO.
[268] Vgl. § 52 StPO.

	Rechtsgrundlage	Bild	Gesprochenes Wort	Biometrische Daten	Standortdaten	Telekomm.-daten	Sonstige
Beschlagnahme	§ 94 StPO	X	X			X	X
Durchsuchung von Wohnungen	§§ 102, 103 StPO						X
Rasterfahndung	§ 98a StPO						X
Lichtbilder	§ 81b StPO	X		X			
Fingerabdruck	§ 81b StPO			X			
DNA	§ 81g StPO			X			
Auskunft Verbindungsdaten	§ 100g StPO					X	
Handyortung	§ 100i StPO				X		
Bildaufnahme	§ 100f StPO	X					
Technische Mittel zur Erforschung des Sachverhalts	§ 100f StPO		X		X		
Telekommunikationsüberwachung	§ 100a StPO		X		X	X	
Abhören des nichtöffentlich gesprochenen Wortes in Wohnungen	§ 100c StPO		X				
Abhören des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen	§ 100f StPO		X				

Tabelle 12: Bereichsspezifische Vorschriften der Strafprozessordnung

Die Rasterfahndung, die Beschlagnahme und die Auskunft über Telekommunikationsdaten stellen einen Zugriff auf durch Dritte erhobene Daten dar. Eine Verknüpfung von Daten findet dabei insbesondere im Rahmen der Rasterfahndung[269] statt. Als Datenbestand kann die Polizei dabei sowohl auf bei Unternehmen verfügbare Daten zurückgreifen als auch auf solche, die von Behörden übermittelt wurden.

3.2.7.4 Verkettung von Daten

Es ist im Hinblick auf Fragen der Verkettung und Verkettbarkeit von Informationen möglich, eine Unterscheidung der polizeilichen Datenerhebung und -verarbeitung dahingehend vorzunehmen, durch wen die im Rahmen der Erkenntnisgewinnung ausgewerteten Daten originär erhoben worden sind. Dies kann entweder durch die Polizei selbst erfolgt sein, oder durch Dritte, insbesondere Unternehmen und Behörden, aber auch Private.

[269] Eine Rasterfahndung ist ein maschineller Abgleich von personenbezogenen Daten, die bestimmte auf einen Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, mit anderen Daten. Dadurch sollen Personen gefunden werden, die für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen, vgl. § 98a StPO.

Die Polizei erhebt Daten selbst, wenn sie durch technische Mittel oder eigene Wahrnehmung der Polizeibeamten Angaben über eine natürliche Person ohne Hinzuziehen eines Dritten beschafft.

Staatsanwaltschaft und Polizei verfügen über eine Reihe von Datenbanken, in denen personenbezogene Daten gespeichert werden und aus denen sich Erkenntnisse über Personen zusammenführen lassen.

Das informationstechnische Verbundsystem INPOL ist ein elektronischer Datenverbund zwischen Bund und Ländern. Eine Zentraldatei wird dabei vom BKA geführt. Die Polizeibehörden der Länder[270] führen eigene Datenbanken. Es gibt zudem Datenbanken des Bundeskriminalamts[271], der Bundespolizei und der Nachrichtendienste[272], die teilweise in der Anti-Terror-Datei[273] zusammengeführt werden.[274]

Durch die Ausweitung der europäischen Zusammenarbeit im Bereich der Polizei und Justiz[275] bietet sich für deutsche Sicherheitsbehörden zunehmend die Möglichkeit, europaweit auf Datenbanken zuzugreifen. Auch deutsche Daten fließen im Rahmen dieses Informationsaustausches ab. Es ist eine zunehmende Proliferation von Daten zu beobachten. Darüber hinaus besteht bereits ein Informationsverbund europäischer Sicherheitsbehörden[276] mit Datenbanken wie EURODAC[277], EUCARIS[278], dem Visa Information System (VIS) und dem Schengener Informationssystem (SIS).

Auf Vorrat werden nach der Umsetzung der EU-Richtlinie 2006/24/EG[279] zur Vorratsdatenspeicherung von Verbindungsdaten zudem deutsche Anbieter von Telekommunikationsdiensten und Internetanbieter Verkehrsdaten und Standortdaten für den Zugriff von Strafverfolgungsbehörden bereithalten müssen.

Technisch bereits möglich sind nicht nur für Geheimdienste, sondern auch für Polizeibehörden intelligente Auswertungen und Analysen von Daten aus vielfältigen Quellen.[280]

3.2.7.5 Folgen für den Betroffenen

Bei Unternehmen sind umfangreiche Daten über Bürger verfügbar, die diese im Rahmen von Vertragsverhältnissen, aufgrund gesetzlicher Erlaubnistatbestände oder aufgrund einer Einwilligung

[270] In Schleswig-Holstein wird das Verfahren INPOL-Land geführt. Zudem gibt es die Fachanwendung @artus.

[271] Eine Übersicht der beim BKA geführten Datenbanken findet sich in der Antwort der Bundesregierung auf die kleine Anfrage der Fraktion DIE LINKE „Möglichkeiten der Zusammenarbeit der Sicherheitsbehörden des Bundes“, BT-Drucksache 16/2875, abrufbar unter http://dip.bundestag.de/btd/16/028/1602875.pdf (letzter Zugriff im Oktober 2007).

[272] Eine Verkettung von nachrichtendienstlichen Daten ist innerhalb der Dienste weitgehend möglich. Die Einführung der Anti-Terror-Datei spiegelt die Tendenz wider, das Trennungsgebot aufzuweichen.

[273] Zur Anti-Terror-Datei [Roggan/Bergemann 2007].

[274] Eine Übersicht der zusammengeführten Dateien findet sich bei c't in dem Artikel „Von der Anti-Terror-Gesetzgebung über die Anti-Terror-Datei zum 'Schäuble-Katalog'“ vom 28.02.2007, abrufbar unter http://www.heise.de/ct/hintergrund/meldung/85995/ (letzter Zugriff im Oktober 2007).

[275] Zum Vertrag von Prüm vgl. [Schaar 2006].

[276] Vgl. [Schaar 2005], abrufbar unter http://files.institut-fuer-menschenrechte.de/488/d48_v1_file_4486915795f82_DIM_MIR_www.pdf (letzter Zugriff im Oktober 2007).

[277] Das europäische dactyloskopische System dient dem Abgleich von Fingerabdrücken von Asylbewerbern und illegalen Einwanderern. Informationen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zu EURODAC sind abrufbar unter http://www.bfdi.bund.de/cln_030/nn_531474/sid_D9696ED12D64AC91B38BDE53BE1A04AC/DE/EuropaUndInternationales/PolZusarb/Artikel/EURODAC.html__nnn=true (letzter Zugriff im Oktober 2007).

[278] European Car Information System.

[279] Richtlinie 2006/24/EG des Europäischen Parlaments über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden.

[280] Eine Darstellung der technisch möglichen und bei der Polizei New Yorks bereits praktizierten Analysen findet sich bei T. J. Lueck: „From Database to Crime Scene: Network is Potent Police Weapon“ in der New York Times vom 07.06.2007, abrufbar unter http://www.nytimes.com/2007/06/07/nyregion/07real.html (letzter Zugriff im Oktober 2007; Subskription erforderlich). Eine Beschreibung von technischen Möglichkeiten findet sich auch bei einem deutschen Anbieter: http://www.rola.com/mod2/branchen/behoerden.html (letzter Zugriff im Oktober 2007).

der Betroffenen erhoben und gespeichert haben. Einen vollständigen Überblick darüber, welche privaten Stellen personenbezogene Daten über eine Person gespeichert hat, ist dem Betroffenen im Bereich der Privatwirtschaft längst nicht mehr möglich. Dabei werden Daten durch Unternehmen verknüpft und angereichert, um zum Beispiel im Rahmen von Customer Relations Management Kundenprofile erstellen oder gezielter werben zu können. Auf diese angereicherten Daten mit unter Umständen hohem Aussagewert über persönliche Präferenzen einzelner Personen haben Strafverfolgungsbehörden im Rahmen von Auskunftsersuchen Zugriff.[281] Betroffen sind zudem auch nicht Beschuldigte wie Hinweisgeber, Zeugen, Opfer oder Angehörige.

Durch die Ausweitung von Eingriffsbefugnissen weit in das Gefahrenvorfeld kann der Einzelne nicht mehr davon ausgehen, dass er grundsätzlich nicht Betroffener von Ermittlungstätigkeiten der Polizei sein wird, solange er dafür keinen Anlass bietet. Im Rahmen der Terrorismusbekämpfung kann mangels Einengung auf einen Kreis möglicher Tatobjekte oder Täter[282] jeder ein Subjekt polizeilicher Verdachtsgewinnungseingriffe werden.

3.2.7.6 Betroffenenrechte

Die Betroffenenrechte auf Auskunft, Berichtigung, Löschung, und Sperrung gelten grundsätzlich auch für die Datenverarbeitung durch die Polizei.

Die Polizeigesetze der Länder sehen zunächst grundsätzlich eine offene Datenerhebung vor. Wenn die Polizei sich mit einem Auskunftsbegehren an einen Betroffenen oder eine einen Dritten wendet, hat sie den Adressaten auf seine Auskunftspflicht oder die Freiwilligkeit der Auskunft hinzuweisen.[283]

Die Strafprozessordnung sieht für viele Ermittlungsmethoden Transparenzregelungen vor, um dem Betroffenen die Möglichkeit zu geben, sich einen Eindruck zu verschaffen, welche Informationen der Staat über ihn erhoben und gespeichert hat. So soll eine Durchsuchung beispielsweise im Beisein des Betroffenen stattfinden. Bei verdeckten Ermittlungen sind Benachrichtigungspflichten nach Abschluss der Maßnahme vorgesehen.[284] Hinsichtlich der vorgesehenen nachträglichen Unterrichtung bestehen in der Praxis erhebliche Defizite.[285]

Dem Betroffenen steht ein Auskunftsanspruch gegenüber der Polizei und Sicherheitsbehörden hinsichtlich der zu seiner Person gespeicherten Daten zu.[286] Der Anspruch kann nur in Ausnahmefällen eingeschränkt werden. Eine Einsicht in Akten darf nicht erfolgen, wenn die Daten mit personenbezogenen Daten Dritter oder geheimhaltungsbedürftigen, nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. Auskunft kann insbesondere verlangt werden über

- die zur Person des Antragstellers gespeicherten Daten,
- den Zweck und die Rechtsgrundlage der Speicherung,
- die Herkunft personenbezogener Daten, die Empfänger von Übermittlungen und die Teilnehmer an automatisierten Abrufverfahren.

Die Pflicht zur Berichtigung von unrichtigen Daten, also solchen, die nicht den tatsächlichen Gegebenheiten entsprechen, ergibt sich für die Polizei teilweise aus den Landespolizeigesetzen, sonst aus dem Bundesdatenschutzgesetz.[287]

---

[281] BVerfG 1 BvR 518/02.

[282] [Bausbach 2006] geht vom Vorliegen einer Dauergefahr aus.

[283] Für Schleswig-Holstein: § 178 Abs. 3 Landesverwaltungsgesetz Schleswig-Holstein.

[284] Ein Gesetzesentwurf zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG sieht Regelungen zum nachträglichen Rechtsschutz für Betroffene vor. Der Regierungsentwurf ist verfügbar unter http://www.bmj.bund.de/files/-/2047/RegE%20TK%DC.pdf (letzter Zugriff im Oktober 2007).

[285] Siehe [Kutscha 2003] und 29. Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Textziffer 4.2.2.

[286] In Schleswig-Holstein ergibt sich dieser aus § 198 Abs. 1 Landesverwaltungsgesetz oder für Auskünfte aus Akten aus § 189 Landesverwaltungsgesetz.

[287] Ausführlich zu Berichtigung und Löschung: [Petri 2007, S. 950 Rn. 388 ff.].

Eine Pflicht zur Löschung von Daten ergibt sich aus bereichsspezifischen Regelungen. Die Polizeigesetze sehen Prüffristen vor, wann die Erforderlichkeit der weiteren Speicherung von personenbezogenen Daten für jeden Fall vorgenommen werden müssen. Nur solange Daten für den festgelegten Zweck erforderlich sind, dürfen sie gespeichert werden. Liegt eine Erforderlichkeit im Zeitpunkt der Prüfung nicht vor, sind die Daten zu löschen. Eine Löschung muss unabhängig von Prüffristen erfolgen, wenn die Polizei feststellt, dass die Speicherung bestimmter Daten unzulässig ist.

3.2.7.7 Fazit

Strafverfolgungsbehörden können im Rahmen ihrer Tätigkeit nicht nur selbst, teilweise verdeckt, umfangreiche personenbezogene Daten erheben, verarbeiten und dabei verknüpfen. Ihnen steht auch die Möglichkeit zu, Zugriff zu nehmen auf bei Unternehmen und Privatpersonen gespeicherte Daten. So ermöglicht heute die Vernetzung technisch nicht nur multiple Verwendungen von Daten, sondern eine unendlich variable Verarbeitung.[288]

3.3 Verhältnis Verbraucher – Unternehmen

3.3.1 Allgemeiner rechtlicher Abriss

3.3.1.1 Rechtsgrundlagen für eine Verkettung personenbezogener Daten

Das Grundrecht der Verbraucher[289] auf informationelle Selbstbestimmung wird gegenüber den Daten verarbeitenden Unternehmen durch das sog. Verbraucherdatenschutzrecht[290] gewährleistet. Dieses ist nicht in einem separaten Spezialgesetz kodifiziert, einschlägig sind hier vielmehr vor allem die Vorschriften des Bundesdatenschutzgesetzes (BDSG), die die Verarbeitung personenbezogener Daten durch private Stellen regeln.[291] Daneben sind aber auch Bestimmungen aus anderen Gesetzen – z.B. dem Bürgerlichen Gesetzbuch (BGB)[292] – zu beachten.

Auch im Verhältnis von Verbraucher und Unternehmen gilt das Verbot mit Erlaubnisvorbehalt, wonach eine Verkettung personenbezogener Daten nur dann zulässig ist, wenn sie aufgrund einer Rechtsvorschrift oder einer Einwilligung des Betroffenen erfolgt.

Eine Verkettung personenbezogener Daten kann also zunächst durch eine Einwilligung des betroffenen Verbrauchers legitimiert werden. Anders als im Verhältnis von Bürger und Staat spielt die Einwilligung bei einer Verkettung personenbezogener Verbraucherdaten durch Unternehmen auch eine wichtige Rolle.

Hat der Verbraucher nicht in die Datenverarbeitung eingewilligt, ist sodann zu prüfen, ob diese durch bereichsspezifische Vorschriften legitimiert wird. Sind solche speziellen Vorschriften nicht einschlägig, ist die Zulässigkeit einer Verkettung personenbezogener Daten an den allgemeinen gesetzlichen Verarbeitungsbefugnissen der §§ 28-30 BDSG zu messen.

---

288 Simitis bei heise online „Innere Sicherheit: Auf der Rutschbahn von Ausnahmegesetzen“, 15.06.2007, abrufbar unter http://www.heise.de/newsticker/meldung/91183/ (letzter Zugriff im Oktober 2007).

289 Nach § 13 BGB ist Verbraucher jede natürliche Person, die ein Rechtsgeschäft zu einem Zwecke abschließt, der weder ihrer gewerblichen noch ihrer selbstständigen beruflichen Tätigkeit zugerechnet werden kann.

290 Ausführliche Ausführungen zum Verbraucherdatenschutzrecht finden sich in der im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft erstellten Studie „Erhöhung des Datenschutzniveaus zugunsten der Verbraucher“ [ULD-Verbraucherdatenschutz-Studie 2006]. Wie sich bereits dem Titel entnehmen lässt, wurden in dieser Studie insbesondere auch Handlungsempfehlungen dafür erarbeitet, wie das bestehende Datenschutzniveau für die Verbraucher zukünftig noch weiter verbessert werden kann.

291 Vgl. insbesondere §§ 28 ff. BDSG.

292 Wird etwa eine datenschutzrechtliche Einwilligung auf der Basis vorformulierter Vertragsklauseln eingeholt, so sind die Vorschriften der §§ 305 ff. BGB, die die Verwendung Allgemeiner Geschäftsbedingungen (AGB) regeln, zu beachten.

3.3.1.1.1 Verkettung(en) aufgrund einer Einwilligung des Verbrauchers

Eine Verkettung personenbezogener Verbraucherdaten durch ein Unternehmen kann also – wie jede andere Datenverarbeitung auch – durch eine Einwilligung des betroffenen Verbrauchers legitimiert werden.

Die gesetzlichen Anforderungen an eine wirksame datenschutzrechtliche Einwilligung finden sich in § 4a BDSG, wonach eine Einwilligung freiwillig, informiert und formgerecht erteilt werden muss. Die Erteilung der Einwilligung muss zudem bereits vor der Datenverarbeitung erfolgen.

Eine wirksame Einwilligung muss zunächst einmal freiwillig sein, d.h. auf der freien Entscheidung des betroffenen Verbrauchers beruhen. Sofern dieser sich in einer Situation befindet, die ihn dazu zwingt, sich mit der Verarbeitung seiner personenbezogenen Daten einverstanden zu erklären, ist eine von ihm erteilte Einwilligung folglich unwirksam.[293] Durch dieses Erfordernis der Freiwilligkeit soll nicht zuletzt verhindert werden, dass eine Daten verarbeitende Stelle die Erbringung einer Leistung von der Einwilligung des Betroffenen in die Verarbeitung solcher Daten abhängig macht, die für die Leistungserbringung nicht benötigt werden. Ausdrücklich gesetzlich geregelt ist dieses sog. Koppelungsverbot im Bereich der Telekommunikation und der Telemedien.[294]

Weitere Voraussetzung einer wirksamen Einwilligung ist die ausreichende Information des Betroffenen. Auf diese Anforderung einer wirksamen Einwilligung wird an anderer Stelle in diesem Grundlagenkapitel noch näher eingegangen.[295]

Eine wirksame Einwilligung liegt darüber hinaus nur dann vor, wenn sie formgerecht erteilt worden ist. Nach § 4a Abs. 1 S. 3 BDSG muss eine Einwilligung grundsätzlich schriftlich erteilt werden. Soll sie zusammen mit anderen Erklärungen abgegeben werden, ist sie besonders hervorzuheben. Die elektronische Form nach § 126a BGB ist der Schriftform gleichgestellt – sie wird allerdings nur dann gewahrt, wenn das elektronische Dokument nicht nur mit dem Namen des Ausstellers, sondern darüber hinaus auch mit einer qualifizierten elektronischen Signatur im Sinne des Signaturgesetzes verbunden ist. Im Bereich von Telekommunikations- und Telemediendiensten ist eine elektronische Einwilligung im Übrigen unter bestimmten Voraussetzungen auch dann zulässig, wenn sie nicht mit einer qualifizierten elektronischen Signatur versehen ist.[296] Ansonsten sind Ausnahmen vom Grundsatz der Schriftlichkeit nur dann zulässig, wenn wegen besonderer Umstände eine andere Form angemessen ist.[297]

Schließlich setzt eine wirksame Einwilligung in die Verarbeitung personenbezogener Daten voraus, dass sie bereits vor Beginn der Datenverarbeitung erteilt worden ist. Ist dies nicht der Fall, so ist eine dennoch durchgeführte Verarbeitung unzulässig. Die Rechtswidrigkeit der Datenverarbeitung kann in einem solchen Fall auch nicht durch eine nachträglich erteilte Einwilligung geheilt werden.[298]

Abschließend sei noch angemerkt, dass Ermächtigungen für eine Verarbeitung personenbezogener Daten, die in Allgemeinen Geschäftsbedingungen enthalten sind, gem. §§ 305 ff. BGB einer besonderen Kontrolle unterliegen.[299]

---

[293] Vgl. Simitis in [Simitis 2006, § 4a Rn. 62].

[294] Gem. §§ 95 Abs. 5 TKG, 12 Abs. 3 TMG darf ein Anbieter von Telekommunikation bzw. von Telemedien die Bereitstellung solcher Dienste nicht von der Einwilligung des Nutzers in eine Verwendung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Diensten nicht oder nur in einer nicht zumutbaren Weise möglich ist.

[295] Hierzu vgl. unten unter 3.3.1.2.

[296] §§ 94 TKG, 13 Abs. 2 TMG. Hiernach muss der Diensteanbieter sicherstellen, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Darüber hinaus finden sich auch in einigen Landesdatenschutzgesetzen vergleichbare Vorschriften (vgl. z.B. § 12 Abs. 3 LDSG SH).

[297] So ist eine mündliche Erteilung der Einwilligung etwa dann zulässig, wenn seitens des Betroffenen eine besondere Eilbedürftigkeit vorliegt.

[298] Simitis in [Simitis 2006, § 4a Rn. 29].

[299] In diesem Zusammenhang ist u.a. zu prüfen, ob solche Klauseln ungewöhnlich und damit für den betroffenen Verbraucher überraschend sind oder ob sie ihn entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Im Rahmen dieser Kontrolle sind auch die wesentlichen Grundgedanken des BDSG zu beachten.

3.3.1.1.2 Verkettung(en) auf Grundlage des § 28 BDSG

Das Bundesdatenschutzgesetz unterscheidet bei den für eine Datenverarbeitung durch nichtöffentliche Stellen in Betracht kommenden gesetzlichen Rechtsgrundlagen zwischen der Verarbeitung als Mittel für die Erfüllung eigener Zwecke und der geschäftsmäßigen Datenspeicherung oder Veränderung zum Zwecke der Übermittlung. Welche dieser beiden Varianten im Einzelfall vorliegt, richtet sich nach der jeweiligen Zweckbestimmung der Datenverarbeitung.

§ 28 BDSG enthält Regelungen für die Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen für eigene – interne – Geschäftszwecke. Die entsprechenden Zulässigkeitstatbestände für eine Datenverarbeitung für eigene Zwecke finden sich in § 28 Abs. 1 BDSG. Entscheidend ist hier stets der im Einzelfall mit der Datenverarbeitung verfolgte Zweck, der bereits bei der Erhebung personenbezogener Daten konkret festgelegt werden muss.[300]

Zentrale Befugnisnorm im Bereich des Verbraucherdatenschutzrechts ist § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wonach eine Verarbeitung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke dann zulässig ist, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient. Dies ist dann der Fall, wenn die Datenverarbeitung entweder selbst Inhalt des Vertrags mit dem Verbraucher ist oder wenn sie für die Abwicklung des jeweiligen Vertrags erforderlich ist.[301] Entscheidend für die Beurteilung, ob ein Erheben, Verarbeiten oder Nutzen von Verbraucherdaten erforderlich ist, ist der konkrete Vertragszweck im Einzelfall. Pauschal lässt sich sagen, dass die Angabe und Verarbeitung von Name und Adresse eines Verbrauchers in der Regel erforderlich sein wird, um den jeweiligen Verbrauchervertrag überhaupt durchführen zu können. Anders ist hingegen etwa die Angabe und Verarbeitung des Geburtsdatums zu beurteilen, das regelmäßig eine Information darstellen wird, die für die Abwicklung des Vertrags nicht benötigt wird.[302]

Darüber hinaus ist eine Verarbeitung personenbezogener Verbraucherdaten nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG auch dann zulässig, wenn sie der Zweckbestimmung eines vertragsähnlichen Vertrauensverhältnisses dient. Ein solches kann zum einen schon vor Abschluss eines Vertrags – und zwar spätestens mit der Aufnahme von Vertragsverhandlungen – entstehen; zum anderen kann es auch nach Beendigung eines Vertrags bestehen, solange Rechte und Pflichten[303] der Vertragspartner noch nachwirken.[304]

Besteht weder ein Verbrauchervertrag noch ein vertragsähnliches Vertrauensverhältnis, so ist die Verarbeitung personenbezogener Verbraucherdaten zur Erfüllung eigener Geschäftszwecke nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, soweit sie zur Wahrung berechtigter Interessen des Unternehmens erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt. Die Vorschrift setzt zunächst also ein berechtigtes Interesse des Unternehmens voraus: Dieses muss nicht rechtlicher Natur sein, sondern kann auch in einem ideellen oder wirtschaftlichen Interesse liegen, solange es sich nur um ein von der Rechtsordnung gebilligtes Interesse handelt.[305] Darüber hinaus muss die Datenverarbeitung zur Wahrung dieses Interesse auch erforderlich sein, d.h., es darf keine objektiv zumutbare Alternative zu ihr geben.[306] Schließlich darf kein Grund zu der Annahme bestehen, dass ein schutzwürdiges Interesse des Verbrauchers an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ob dies der Fall ist, hängt von einer Abwägung der beiderseitigen Interessen im Einzelfall ab.[307] Bestehen

[300] § 28 Abs. 1 S. 2 BDSG.

[301] Das Wort „dienen“ wird in der Datenschutzliteratur unterschiedlich ausgelegt, wobei die Ansicht, die auf die Erforderlichkeit der Datenverarbeitung abstellt, nach [Gola/Schomerus, § 28 Rn. 13] als herrschend bezeichnet werden kann.

[302] [ULD-Verbraucherdatenschutz-Studie 2006, S. 22].

[303] Hier ist insbesondere die gegenseitige Rücksichtnahmepflicht zu nennen, die sich regelmäßig auch auf die nachvertragliche Zeit auswirkt.

[304] Simitis in [Simitis 2006, § 28 Rn. 121, 123].

[305] [Gola/Schomerus 2005, § 28 Rn. 33].

[306] Simitis in [Simitis 2006, § 28 Rn. 143]. Eine solche zumutbare Alternative besteht z.B. dann, wenn das berechtigte Interesse des Unternehmens an einer Verarbeitung personenbezogener Daten auch durch eine Verarbeitung anonymisierter Daten realisiert werden könnte.

[307] Hier spielen insbesondere Faktoren wie Art und Umfang der Daten, Zahl der Betroffenen, Speicherungsdauer, Verwendungszwecke und Verkettungsmöglichkeiten eine Rolle.

Zweifel, ob die schutzwürdigen Interessen des betroffenen Verbrauchers das berechtigte Interesse des Unternehmens überwiegen, muss dieses auf die geplante Verarbeitung personenbezogener Daten verzichten.[308]

Nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG ist die Verarbeitung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke schließlich dann zulässig, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte. Dies gilt allerdings dann nicht, wenn ein schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Datenverarbeitung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

3.3.1.1.3 Verkettung(en) auf Grundlage des § 29 BDSG

Während § 28 BDSG Regelungen zur Verarbeitung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke enthält, finden sich in § 29 BDSG Bestimmungen zur Zulässigkeit der geschäftsmäßigen Datenerhebung und -verarbeitung zum Zweck der Übermittlung. Konkret geht es also um die Tätigkeit von Kreditinformationssystemen, Handelsauskunfteien, Adresshändlern oder brancheninternen Warndiensten – als Veranschaulichungsbeispiel sei hier die SCHUFA Holding AG (Schutzgemeinschaft für allgemeine Kreditsicherung) genannt. Zu einer Verkettung personenbezogener Daten kann es hier zum einen beim Aufbau entsprechender Datenbanken durch solche Unternehmen kommen, zum anderen können deren Kunden die an sie übermittelten Daten mit ihren bereits existenten Datenbeständen verketten.

Das Gesetz unterwirft diese Art der geschäftsmäßigen Datenverarbeitung in § 29 BDSG besonderen Zulässigkeitsvoraussetzungen, die an dieser Stelle allerdings nicht im Einzelnen vorgestellt werden sollen.

3.3.1.2 Transparenz hinsichtlich der Verkettung von Verbraucherdaten

Ein elementares Prinzip des Datenschutzrechts ist der sog. Transparenzgrundsatz, zu dessen Verwirklichung der verantwortlichen Stelle bestimmte Pflichten auferlegt und dem Betroffenen entsprechende Ansprüche zugebilligt werden: Um eine transparente Verarbeitung personenbezogener Daten sicherzustellen, werden den Daten verarbeitenden Stellen qua Gesetz Informations-, Unterrichtungs- und Benachrichtigungspflichten auferlegt.

Soll eine Datenverarbeitung auf der Grundlage einer Einwilligung des Betroffenen erfolgen, so muss dieser hierüber gem. § 4a Abs. 1 Satz 2 BDSG rechtzeitig und umfassend informiert werden. Die verantwortliche Stelle ist zwar primär dazu verpflichtet, den Betroffenen auf den vorgesehenen Verwendungszweck hinzuweisen, sie darf sich aber nicht hierauf beschränken. Vielmehr muss der Betroffene auch alle Informationen erhalten, die er benötigt, um Anlass, Ziel und Folgen der geplanten Verarbeitung beurteilen zu können.[309] Hierzu muss der Verbraucher zunächst einmal wissen, auf welche personenbezogenen Daten sich seine Einwilligung bezieht.[310] Außerdem müssen auch die im konkreten Fall gegebenen Verarbeitungsbedingungen, potenzielle Übermittlungsempfänger und ggf. auch die mit einer Übermittlung von Daten in unsichere Drittstaaten außerhalb der Europäischen Union verbundenen Risiken offengelegt werden. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen muss der Verbraucher außerdem auch auf die Folgen einer Verweigerung der Einwilligung hingewiesen werden. Schließlich muss der betroffene Verbraucher in einer Art und Weise informiert werden, die für ihn verständlich ist.[311]

Wird die Verarbeitung personenbezogener Daten hingegen durch eine Rechtsvorschrift legitimiert, so differenziert das Gesetz danach, ob die Erhebung personenbezogener Daten mit oder ohne Kenntnis des Betroffenen erfolgt.[312] Bei einer Datenerhebung ohne Kenntnis des Betroffenen ist dieser nach § 4 Abs. 3 Satz 1 BDSG über die Identität der verantwortlichen Stelle, die Zweckbestimmung der

[308] Simitis in [Simitis 2006, § 28 Rn. 166].
[309] Simitis in [Simitis 2006, § 4a Rn. 70].
[310] [Gola/Schomerus 2005, § 4a Rn. 11].
[311] Simitis in [Simitis 2006, § 4a Rn. 72].
[312] Nach dem sog. Grundsatz der Direkterhebung des § 4 Abs. 2 S. 1 BDSG müssen Daten in der Regel beim Betroffenen erhoben werden.

Erhebung, Verarbeitung oder Nutzung und die Kategorien von Empfängern zu unterrichten – Letzteres allerdings nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss. Erfolgt die Erhebung personenbezogener Daten hingegen ohne Kenntnis des Betroffenen, so ist der Betroffene gem. § 33 Abs. 1 BDSG nachträglich von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen.

Den genannten Pflichten der verantwortlichen Stelle korrespondiert der in § 34 BDSG geregelte Anspruch des Betroffenen auf Auskunft.[313] Hiernach kann dieser unentgeltlich Auskunft über die zu seiner Person gespeicherten Daten, die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden und den Zweck der Speicherung verlangen. Im Übrigen stehen dem Betroffenen gem. § 35 BDSG unter bestimmten Voraussetzungen auch Ansprüche auf Berichtigung, Löschung oder Sperrung von Daten zu.

3.3.1.3 Fazit

Im Verhältnis von Verbraucher und Unternehmen finden die einschlägigen Vorschriften des Bundesdatenschutzgesetzes Anwendung. In vielen Fällen wird eine Verarbeitung personenbezogener Daten von Verbrauchern auf der Grundlage einer Einwilligung erfolgen, die nur dann wirksam ist, wenn sie informiert und freiwillig erteilt wird. Zentrale gesetzliche Grundlage einer Verarbeitung von Verbraucherdaten ist § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Diese Regelung legitimiert eine Verarbeitung insbesondere dann, wenn sie Inhalt eines Verbrauchervertrags ist und für die Abwicklung eines solchen Vertrags erforderlich ist. Die Transparenz der Datenverarbeitung soll einerseits durch Informations-, Unterrichtungs- und Benachrichtigungspflichten der verantwortlichen Stelle und andererseits durch das Recht des betroffenen Verbrauchers auf Auskunft sichergestellt werden.

3.3.2 Elektronische Zahlungssysteme

Elektronische Zahlungssysteme sollen die Bezahlung von Waren im Internet ermöglichen, ohne dass dafür physisches Geld bzw. andere physische Nachweise (unterschriebene Belege etc.) benötigt werden. Es ist dafür notwendig, dass Sicherheitseigenschaften von physischem Geld ebenso in der virtuellen Welt durchgesetzt werden können. In [Kang/Lee 2005] werden Anforderungen an elektronisches Geld im Vergleich zu Eigenschaften von physischem Geld beschrieben. Die wichtigsten dieser Eigenschaften sollen hier kurz aufgezählt werden:

- *Anonymität:* Physisches Geld ermöglicht es dem Nutzer, bezüglich der Nutzung des Geldes anonym zu bleiben, da das Geld keine Merkmale besitzt, die es unmittelbar dem Nutzer zuordnen. Elektronisches Geld sollte daher ebenso eine anonyme Nutzung ermöglichen.
- *Teilbarkeit:* Physisches Geld hat eine kleinste Einheit, und es kann entsprechen geteilt bzw. gewechselt werden. Elektronisches Geld sollte daher ebenso teilbar sein.
- *Transferierbarkeit*: Physisches Geld kann an Dritte weitergegeben werden, ohne die Nutzbarkeit des Geldes in irgendeiner Wiese einzuschränken. Elektronisches Geld muss also ebenso übertragen werden können.
- *Verhinderung der Doppelnutzung:* Physisches Geld kann nur einmal ausgegeben werden. Um dies sicherzustellen wird das Fälschen mit diversen Maßnahmen erschwert. Die dem elektronischen Geld zugrundeliegenden Informationen können grundsätzlich einfach kopiert werden. Ein elektronisches Zahlungssystem muss deshalb Maßnahmen und Protokolle benutzten, die es ermöglichen, die mehrfache Benutzung von elektronischem Geld erkennen, verhindern und evtl. bestrafen zu können.

Nach [Asokan et al. 1997] sind an einem elektronischen Zahlungssystem im Allgemeinen vier Parteien beteiligt: Die Bank des Zahlenden als Aussteller der elektronischen Zahlungsmittel, der Zahlende (der

[313] Wie bereits erwähnt, findet sich in § 13 Abs. 7 TMG eine Spezialregelung, wonach ein unter Pseudonym handelnder Nutzer von Telemediendiensten auch Auskunft über die zu seinem Pseudonym gespeicherten Daten verlangen kann.

Sender der Zahlung), der Empfänger der Zahlung, sowie die Bank des Empfängers, die die empfangenen Zahlungsmittel einlöst. Es können grundsätzlich zwei Kategorien unterschieden werden:

1. In *Bargeld-artigen Systemen* wird vom Konto des Zahlenden zunächst ein Geldbetrag abgehoben, den dieser später für Zahlungen verwenden kann. Erhält der Empfänger einen Geldbetrag, kann er diesen auf sein Konto bei seiner Bank einzahlen.
2. Bei *Scheck-artigen Systemen* wird zwischen Sender und Empfänger eine Art „Formular" (das z.B. einem Scheck oder einer Überweisung entspricht) ausgetauscht. Die eigentliche Übertragung des Geldes wird direkt zwischen der Bank des Senders und des Empfängers ausgeführt.

Weiterhin differenziert man zwischen *Online*- und *Offline-Systemen*:

1. In *Online-Systemen* ist an der Ausführung einer Transaktion immer eine dritte Partei (üblicherweise die Bank des Senders oder des Empfängers) als Autorisierungsinstanz beteiligt. Diese Instanz stellt sicher, dass die Transaktion korrekt durchgeführt wird.
2. In *Offline-Systemen* kann eine Transaktion ohne direkte Beteiligung einer solchen Instanz durchgeführt werden. Die Korrektheit der Transaktion (insbesondere die Verhinderung der Doppelnutzung) muss in solchen Systemen entweder durch manipulationssichere Hardware sichergestellt werden, oder die Protokolle müssen so gestaltet sein, dass inkorrektes Verhalten im Nachhinein mit Sicherheit erkannt und bestraft werden kann.

Neben diesen Unterschieden in der Funktionsweise der Zahlungssysteme ist auch deren Einsatzgebiet sehr variabel. So gibt es zum einen universelle Zahlungssysteme, deren Einsatzgebiet dem des herkömmlichen Geldes entspricht. Mit solchen Zahlungssystemen können beliebige Waren bezahlt werden. Zum anderen existiert eine Vielzahl von eingeschränkten Zahlungssystemen, die nicht unmittelbar als solche wahrgenommen werden, da sie im Wesentlichen Gutscheine, z.B. Bonuspunkte, transferieren, die dann in einem mehr oder weniger speziellen Kontext als „Bezahlung" verwendet werden können.

Bezüglich Verkettbarkeit sind bei elektronischen Zahlungssystemen zwei Aspekte interessant: Zum einen ist dies die oben bereits beschriebene Anonymität des Senders vor dem Empfänger. Zum anderen können Protokolle so gestaltet werden, dass unterschiedliche Transaktionen unverkettbar sind, d.h., dass ein Empfänger (und evtl. auch seine Bank) nicht erkennen kann, ob Transaktionen vom selben Sender ausgehen.

Falls ein Zahlungssystem die Verkettbarkeit von Transaktionen nicht verhindert, sind Verkettungen allerdings unmittelbar nur in jeweiligen Anwendungsbereich des Systems möglich. Universelle Zahlungssysteme haben dementsprechend ein größeres Potenzial für die Bildung umfassender Nutzerprofile als eingeschränkte Zahlungssysteme.

Im heutigen Internethandel werden in überwiegendem Maße herkömmliche Zahlungsmethoden eingesetzt (Vorauskasse, Rechnung, Nachnahme, Kreditkarte). Obwohl eine Vielzahl alternativer Anbieter für speziell auf das Internet ausgelegter Bezahlmethoden existiert, wird lediglich das Bezahlverfahren des Anbieters PayPal in größerem Umfang benutzt (u.a. [Heng 2007][314]). Detaillierte Auswertungen zu Zahlungsabwicklungen im Internet finden sich in [Stahl et al. 2006]. Untersuchungen zu Sicherheitseigenschaften, u.a. zur Anonymität des Kunden gegenüber dem Händler können in [Stahl et al. 2005] nachgelesen werden.

[314] Abrufbar unter http://www.ecin.de/state-of-the-art/bezahlsysteme/ (letzter Zugriff im Oktober 2007).

3.3.3 Erstellung von Kundenprofilen durch Unternehmen („Profiling“)

3.3.3.1 Grundsätzliche Erläuterung des Begriffs Profiling

„Profiling“ bezeichnet eine Vielzahl an Verfahren, die alle darauf abzielen, aus aggregierten Datenbeständen nutzbare Informationen zu destillieren[315]. Anders formuliert zielt jedes Profiling darauf ab, aus einer Fülle von – für sich genommen oftmals belanglosen – Daten verwertbares Wissen abzuleiten. Profiling umfasst sowohl die Erstellung als auch die Nutzung von Profilen.[316] Dabei wird sich ein Profiling in vielen Fällen auf eine Einzelperson oder eine Gruppe von Personen beziehen, es können aber auch Profile zu Organisationen, Dingen oder Ereignissen erstellt werden. Hierfür werden üblicherweise Methoden wie Data Warehousing und Data Mining verwendet.

Der Begriff *Data Warehouse* bezeichnet dabei ein Konzept, das darauf gerichtet ist, eine zentrale Datenbank mit allen in einer Organisation vorhandenen Daten aufzubauen, um sie dann jederzeit aus dieser Datenbank abrufen und für verschiedene Zwecke nutzen zu können.[317] Ein Data Warehouse ist eine hervorragende Voraussetzung für ein effektives *Data Mining*, das verschiedene Verfahren zur Analyse komplexer Datenbestände mittels Algorithmen bezeichnet und dessen Ziel es ist, verborgene Muster oder Trends aufzudecken und so neue Wissenszusammenhänge zu generieren.[318] Ein mit Hilfe solcher Verfahren erstelltes Profil bietet dann nicht nur die Summe der einzelnen Informationen, es ermöglicht vielmehr regelmäßig auch die Gewinnung neuer Erkenntnisse in Gestalt sog. Meta-Informationen.

Generiert und genutzt werden entsprechende Profile sowohl von hoheitlichen als auch von privaten Stellen. Im staatlichen Bereich findet Profiling etwa in der Kriminalistik, in Gestalt der Rasterfahndung oder bei der Erstellung und Auswertung amtlicher Statistiken statt. Als Beispiele für ein Profiling im Bereich der Privatwirtschaft seien an dieser Stelle nur die Erstellung und Nutzung von Kundenprofilen, die in diesem Abschnitt im Fokus der Betrachtungen stehen, sowie der Spezialfall der Verwendung sog. Scoring-Verfahren[319] genannt. Wie bereits diese wenigen Beispiele deutlich machen, umfasst „Profiling“ also eine große Anzahl an oftmals recht heterogen ausgestalteten Methoden und Verfahren.

Gemeinsam ist all diesen verschiedenen Varianten des Profilings jedoch das Ziel der Wissensgenerierung.[320] Werden Profile zu natürlichen Personen erstellt, besteht die Zielsetzung überwiegend darin, ein künftiges Verhalten dieser Datensubjekte und hiermit einhergehende Chancen (z.B. Absatzsteigerung durch den Verkauf von Produkten) oder Risiken (z.B. Ausfall eines gewährten Kredits) zu prognostizieren. Da also die (Teil-)Identität einer Person durch eine Erstellung von Profilen in vielerlei Hinsicht näher beleuchtet werden kann, handelt es sich beim Profiling um einen der drei grundsätzlichen Typen des Identitätsmanagements (Typ 2-IMS, vgl. [Bauer/Meints/Hansen 2005] sowie Abschnitt 4.6).

Wie bereits gesehen, unterscheiden sich Profile zunächst einmal danach, von wem, über wen oder was und zu welchem Zweck sie erstellt werden. Darüber hinaus lassen sich aber noch weitere bzw. verfeinerte Arten und Kategorien von Profiling identifizieren, über die an dieser Stelle ein kurzer Überblick gegeben wird:

Profile können manuell oder automatisiert erstellt werden[321], wobei nachfolgend ausschließlich automatisiert generierte Profile im Fokus der Betrachtungen stehen werden. Bei einer solchen automatisierten Erstellung von Profilen kommen im Übrigen nicht nur bestimmte Techniken (im Sinne von

[315] Einzelheiten zum Begriff und zu den unterschiedlichen Arten des Profilings finden sich bei [Hildebrandt/Backhouse 2005]. Eine Zusammenfassung der innerhalb des FIDIS-Projekts erzielten Ergebnisse gibt [Hildebrandt 2006].
[316] Vgl. [Hildebrandt/Backhouse 2005, S. 12].
[317] Vgl. Scholz in [Roßnagel 2003, Kap. 9.2 Rn. 3].
[318] Scholz a.a.O.
[319] Näheres hierzu siehe die Ausführungen in Abschnitt 3.3.4 zu Scoring-Verfahren.
[320] [Hildebrandt/Backhouse 2005, S. 13 f.].
[321] [Hildebrandt/Backhouse 2005, S. 14 f.].

Verfahren oder Methoden), sondern auch entsprechende Technologien (Hard- und Software) zum Einsatz.

Des Weiteren kann bei Profilen zu Personen danach differenziert werden, ob sie deren Offline- und/oder Online-Verhalten betreffen.[322] Im Internetzeitalter kommt dem Surfverhalten („clickstream“) von Nutzern ein immer größere Bedeutung zu[323] – RFID und Ubiquitous Computing werden zukünftig aber auch die einfache Erstellung umfassender (digitaler) Profile des Offline-Verhaltens von Personen technisch möglich machen.

Darüber hinaus lassen sich noch personalisierte und Gruppenprofile unterscheiden[324]: Personalisierte Profile identifizieren und repräsentieren eine Person und beschreiben einige ihrer Attribute. Gruppenprofile erfüllen die gleiche Funktion hinsichtlich einer Gruppe. Bei dieser kann es sich um eine Gemeinschaft, deren Mitglieder sich ihr zugehörig fühlen, oder schlicht um eine bestimmte Kategorie von Menschen (z.B. Linkshänder) handeln. Gruppenprofile können distributiv oder nicht-distributiv sein[325]: Eine distributive Gruppe zeichnet sich dadurch aus, dass die Attribute der Gruppe zugleich auch Attribute eines jeden Mitglieds dieser Gruppe sind. Charakteristisch für eine nicht-distributive Gruppe ist hingegen, dass die Gruppenattribute nicht bei allen Mitgliedern, sondern nur bei einem gewissen Prozentsatz vorliegen. Hier besteht also die Gefahr, dass einem Mitglied der Gruppe aufgrund einer Wahrscheinlichkeitsprognose ein bestimmtes Attribut zugeordnet wird, obwohl dieses bei ihm in Wirklichkeit überhaupt nicht vorliegt.

Abschließend sei bemerkt, dass bei der Erstellung von Profilen oftmals ein Mangel an Transparenz besteht. Vielfach ist der analysierten Person schon nicht bewusst, dass überhaupt ein Profil über sie erstellt wird. In vielen anderen Fällen weiß sie dies zwar, wird aber nicht darüber informiert, welche Daten für das jeweilige Profiling verwendet werden und nach welchen Kriterien diese Daten ausgewertet werden.[326]

3.3.3.2 Erstellung und Auswertung von Kundenprofilen durch Unternehmen

3.3.3.2.1 Verkettung von Verbraucherdaten zu Profilen

Im Bereich der Privatwirtschaft ist das Verketten von Daten zu Kundenprofilen seit einigen Jahren gängige Praxis. Unternehmen nutzen solche – fortlaufend aktualisierten – Kundenprofile dazu, aus ihnen Verhaltensmuster abzuleiten und künftiges Verhalten von Verbrauchern zu prognostizieren. Ziel ist es, die auf diese Weise gewonnenen Erkenntnisse zum Vorteil des Unternehmens zu nutzen. Ermöglicht werden insoweit nicht nur personalisierte Werbung und Preisdiskriminierung; die generierten Meta-Informationen können vielmehr – wie etwa beim unternehmensinternen Scoring – auch zur Risikominimierung oder zu Zwecken der Marktforschung verwendet werden. Je mehr Einzelangaben über einen Kunden in sein Profil Eingang finden, umso aussagekräftiger ist dieses.

Private Unternehmen haben folglich ein großes kommerzielles Interesse an einer Erstellung umfangreicher Kundenprofile, die ein möglichst detailliertes Bild der jeweiligen Person ergeben.

3.3.3.2.2 Verkettete Informationen

Zur Erstellung von Kundenprofilen werden Kundenstammdaten (wie Name, Adresse und Geburtsdaten) mit Informationen zum Konsumverhalten der jeweiligen Person verkettet.[327] Diese unternehmenseigenen Datenbestände werden vielfach noch durch von außen zugekaufte Informationen (z.B.

[322] [Hildebrandt/Backhouse 2005, S. 15 f.].
[323] Ausführlich mit diesem Themenkomplex befasst sich etwa [Schaar 2001].
[324] Hierzu [Hildebrandt 2006, S. 549 f.].
[325] [Hildebrandt/Backhouse 2005, S. 30 f.].
[326] Die Offenlegung von Kriterien wird dabei von Unternehmen regelmäßig mit der Begründung verweigert, bei diesen handele es sich um Betriebs- und Geschäftsgeheimnisse.
[327] Hierzu [ULD-Verbraucherdatenschutz-Studie 2006, S. 31 f.].

branchenspezifische Fachinformationen oder Geodaten) ergänzt.[328] Eine wichtige Rolle bei der Erstellung von Kundenprofilen spielen außerdem sog. Kundenbindungsprogramme, durch die sich eine Vielzahl an Daten über das Konsumverhalten eines Kunden generieren lässt.[329] Unter Verwendung von Techniken und Methoden wie Data Warehousing und Data Mining werden die genannten Einzelinformationen, die isoliert betrachtet überwiegend als harmlos zu beurteilen sind, zu einem umfassenden Profil verdichtet.

Tabelle 13 gibt einen – bei weitem nicht abschließenden – Überblick darüber, welche Daten typischerweise von Unternehmen zur Erstellung von Kundenprofilen genutzt und folglich miteinander verkettet werden:

Kundenstammdaten		
Vor- und Nachname	Adresse	Geburtsdaten
Informationen zum Konsumverhalten		
gekaufte Produkte	Ort des Kaufs	Zeitpunkt des Kaufs
insbesondere: Informationen aus Kundenbindungsprogrammen		
Zugekaufte Informationen		
branchenspezifische Informationen	Geoinformationen	etc.

Tabelle 13: Daten, die typischerweise Eingang in Kundenprofile finden

3.3.3.2.3 Rechtsgrundlagen für eine Erstellung von Kundenprofilen

Sofern Unternehmen personalisierte Profile zu einzelnen Kunden erstellen, weisen die hierbei verketteten Daten überwiegend einen Personenbezug auf. Werden personenbezogene Daten zu Profilen verkettet, liegt regelmäßig ein Verändern dieser Daten im Sinne des § 3 Abs. 4 Nr. 2 BDSG vor, das an den Vorschriften des geltenden Datenschutzrechts zu messen ist.

Vorab sei hier angemerkt, dass dem Bundesverfassungsgericht zufolge eine absolute Obergrenze jeder Datenverarbeitung im Verbot der Erstellung umfassender Persönlichkeitsprofile liegt. Das Gericht hält es für nicht mit der Menschenwürde vereinbar, „den Menschen in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren.[330]“ Dieses Verbot gilt nicht nur gegenüber staatlichen Stellen, sondern findet auch im privaten Bereich Anwendung. Praktisch gestaltet sich allerdings die Grenzziehung zwischen erlaubten Datensammlungen zu einer bestimmten Person und unzulässigen Persönlichkeitsprofilen außerordentlich schwierig.[331] Da bei der Erstellung von Kundenprofilen neben bestimmten Basisdaten „nur“ Informationen zum Konsumverhalten der jeweiligen Person gespeichert werden, dürfte hier die soeben skizzierte Obergrenze in aller Regel nicht überschritten werden.[332]

Aus der Sicht von Unternehmen stellt sich damit die Frage, auf welcher Rechtsgrundlage und unter welchen Voraussetzungen eine Erstellung von Kundenprofilen zulässig ist.[333]

In diesem Zusammenhang ist zunächst festzustellen, dass § 28 Abs. 1 Nr. 1 BDSG als Rechtsgrundlage für die Erstellung von Kundenprofilen ausscheidet, da eine Verkettung von Daten zu Kundenprofilen nicht für eine Abwicklung von Verbraucherverträgen erforderlich ist. Auch eine Legitimation der Erstellung von Kundenprofilen durch § 28 Abs. 1 Nr. 2 BDSG scheidet in aller Regel aus: Zwar haben Unternehmen ein – grundsätzlich legitimes – wirtschaftliches Interesse an der Auswertung

[328] Auf die mit einem solchen Handel mit Persönlichkeitsprofilen verbundenen rechtlichen Fragestellungen soll an dieser Stelle nicht näher eingegangen werden. Ausführlich beleuchtet werden sie etwa von [Moos 2006].
[329] Näheres hierzu im Abschnitt 3.3.5.
[330] BVerfGE 65, 1 (52).
[331] Hierzu Weichert in [Däubler et al. 2007, Einl. Rn. 42].
[332] So auch [ULD-Kundenbindungsstudie 2003, S. 45].
[333] Vgl. hierzu [ULD-Verbraucherdatenschutz-Studie 2006, S. 32 f.].

solcher Profile, in den meisten Fällen wird aber das Interesse des Betroffenen am Schutz seiner Privatsphäre und seines Persönlichkeitsrechts das Interesse des Unternehmens an der Erstellung des Profils überwiegen. Dies gilt jedenfalls für den Regelfall, dass ein Kundenprofil zur Gewinnung von Meta-Informationen verwendet wird.[334]

In den meisten Fällen kommt als Rechtsgrundlage für eine Erstellung von Kundenprofilen also nur eine Einwilligung der betroffenen Verbraucher in Betracht.[335]

Problematisch ist in diesem Zusammenhang allerdings, dass der genaue Zweck der Erstellung von Kundenprofilen vielfach erst nach deren Auswertung festgestellt werden kann. Oftmals geht es schließlich darum, durch die Auswertung von Kundenprofilen neue Erkenntnisse zu gewinnen, die zuvor keine der in dem jeweiligen Unternehmen involvierten Personen überhaupt nur in Betracht gezogen hat. Im Hinblick auf die Wirksamkeit einer Einwilligung ist also stets zu prüfen, ob der Verwendungszweck der Kundenprofile genau genug spezifiziert worden und der Kunde über diesen Zweck sowie über alle weiteren wesentlichen Umstände ausreichend informiert worden ist.

Schließlich ist noch zu beachten, dass eine Einwilligung oftmals durch die Unterzeichnung entsprechender Allgemeiner Geschäftsbedingungen erfolgen wird. Ist dies der Fall, so ist sie an den Vorschriften der §§ 305 ff. BGB zu messen und kann hiernach insbesondere dann unzulässig sein, wenn der entsprechende Passus gem. § 305 c Abs. 1 BGB als überraschende Klausel zu beurteilen ist oder wenn eine Klausel den Verbraucher gem. § 307 Abs. 1 Satz 1 BGB entgegen den Geboten von Treu und Glauben unangemessen benachteiligt. Ob dies der Fall ist, muss in jedem Einzelfall sorgfältig geprüft werden.

3.3.3.2.4 Folgen einer Verkettung von Daten zu Kundenprofilen

Mit Hilfe von Kundenprofilen können Unternehmen auf verschiedene Attribute von Kunden wie z.B. Interessenschwerpunkte, Bonität oder seine „Wertigkeit“ im Vergleich zu anderen Kunden schließen. Entsprechende Schlussfolgerungen können sich auf die Behandlung des Kunden durch das Unternehmen auswirken: Im günstigsten Fall wird dem Kunden eine Vorzugsbehandlung zuteil werden, in weniger günstigen Fällen wird ihm beispielsweise ein Kredit verweigert werden oder ein Angebot erst gar nicht unterbreitet werden.[336] Damit bleibt an dieser Stelle festzuhalten, dass die Erstellung und Auswertung von Kundenprofilen sich nicht zwangsläufig zum Nachteil eines Kunden auswirken muss, auch wenn dies in vielen Konstellationen der Fall sein wird.

Kundenprofile bieten im Übrigen – insbesondere bei einer Auswertung mittels Data-Mining-Techniken – vielfach die Möglichkeit, (sensible) Zusatzinformationen über einen Kunden zu erlangen. Dieser Umstand wird dem jeweiligen Verbraucher in vielen Fällen jedoch gerade nicht bewusst sein.

3.3.3.2.5 Transparenz

Wie bereits erwähnt, muss der Verbraucher vor Erteilung seiner Einwilligung gem. § 4a Abs. 1 Satz 2 BDSG umfassend über die Modalitäten der Erstellung und Auswertung des geplanten Kundenprofils informiert werden. Er ist also insbesondere darauf hinzuweisen, welche Daten in ein solches Kundenprofil einfließen sollen und zu welchem Zweck das Profil ausgewertet werden soll. Zudem kann der Verbraucher nach Erstellung des Kundeprofils gegenüber dem Unternehmen auch seinen Auskunftsanspruch gem. § 34 BDSG geltend machen.

Entgegen der skizzierten gesetzlichen Verpflichtungen wird der Verbraucher in der Praxis in vielen Fällen wohl schon gar nicht erst darüber informiert werden, dass überhaupt ein Kundenprofil über ihn erstellt wird. Darüber hinaus ist zu befürchten, dass Profile nicht nur für den ursprünglich angegebenen, sondern auch für weitere Zwecke ausgewertet werden.

[334] Siehe hierzu [ULD-Kundenbindungsstudie 2003, S. 45 f.].
[335] So auch [Gola/Schomerus 2005, § 28 Rn. 12] und [ULD-Verbraucherdatenschutz-Studie 2006, S. 33].
[336] [ULD-Kundenbindungsstudie 2003, S. 46].

3.3.3.3 Fazit

Ziel eines jeden Profiling ist es, aus Datenbeständen verwertbare Informationen zu destillieren. Private Unternehmen haben ein vitales wirtschaftliches Interesse an einer Verkettung personenbezogener Daten zu Kundenprofilen, um möglichst viel über Eigenschaften, Verhältnisse und Verhaltensweisen ihrer Kunden zu erfahren. Verkettet werden insoweit Kundenstammdaten, Daten zum Konsumverhalten sowie ggf. freiwillige oder von außen zugekaufte Angaben. Aus datenschutzrechtlicher Sicht ist dies nur dann zulässig, wenn der betroffene Kunde seine Einwilligung zur Erstellung eines solchen Profils erteilt hat.

3.3.4 Scoring-Verfahren

3.3.4.1 Einleitung – Erläuterung des Begriffs Scoring

Der aus dem Englischen stammende Begriff „Scoring“ bedeutet „rechnen, zählen, einstufen, Punkte machen“. Darunter ist im vorliegenden Zusammenhang die statistische Erstellung von Prognosen menschlichen Verhaltens zu verstehen. Nach der ausführlichen Definition im [ULD-Scoring-Gutachten 2006] bezeichnet Scoring „systematische, i.d.R. auf mathematisch-statistischer Analyse von Erfahrungswerten aus der Vergangenheit basierende Verfahren zur Prognose über das zukünftige Verhalten von Personengruppen und Einzelpersonen mit bestimmten Merkmalen.“

Es werden also zunächst bestimmte Merkmale einer Vielzahl von Personen statistisch ausgewertet, um festzustellen, ob zwischen den Merkmalen und bestimmten Verhaltensweisen der Personen statistische Zusammenhänge bestehen. Im Anschluss hieran werden die einzelnen Merkmale entsprechend den zuvor ermittelten Korrelationen im Hinblick auf das zu prognostizierende Verhalten unterschiedlich gewichtet. Nach Abschluss dieser Analyse können einzelne Personen anhand der bei ihnen vorhandenen Ausprägungen der relevanten Merkmale je nach den im Rahmen der Auswertung ermittelten Gewichtungen bewertet werden. Dabei wird aus der Summe der bei einer Person vorhandenen Merkmalswerte der sog. *Score-Wert* (oder kurz „Score“) ermittelt. Dem Score-Wert bzw. einer Score-Wert-Gruppe wird dann schließlich ein Wahrscheinlichkeitswert zugeordnet, der eine Prognose für ein bestimmtes künftiges Verhalten der jeweiligen Person ausdrückt.

Legt man die soeben genannte Definition zugrunde, so kann Scoring in einer Vielzahl von Bereichen eine Rolle spielen, weil es sich bei dem zu prognostizierenden Verhalten um jedes denkbare menschliche Verhalten handeln kann.[337] So ist es beispielsweise möglich, Scoring-Verfahren zur Prognose von Arbeitsleistungen von Beschäftigten oder zur Voraussage terroristischen oder kriminellen Verhaltens einzusetzen. Auch wird mittlerweile im Bereich der gesetzlichen Krankenversicherung darüber nachgedacht, auf der Grundlage der über die Versicherten vorliegenden Daten zu Krankheiten etc. individuelle Score-Werte zu berechnen (sog. Gesundheits-Score).[338] Fasst man den Begriff des Scorings noch weiter, so unterfallen ihm nicht nur Verfahren zur Prognose eines künftigen menschlichen Verhaltens; vielmehr können entsprechende Methoden etwa auch zur (nachträglichen) repressiven Aufklärung von Straftaten eingesetzt werden. Als Beispiele lassen sich die Ermittlungsmethode der Rasterfahndung oder die Rasterung von Finanzdaten zum Aufspüren von Geldwäsche-Verdächtigen nennen.

Vorliegend steht das Verhältnis von Verbrauchern und Unternehmen im Fokus der Betrachtungen.[339] Hier sind verschiedene Arten des Scorings zu unterscheiden:

Das sog. Werbe-Scoring dient der individuellen Ansprache und Bewerbung von Kunden („One-to-One-Marketing“). So kann der jeweils erzielte Score-Wert etwa von Bedeutung für die Entscheidung sein, ob ein Kunde überhaupt beworben werden soll, mit welchen Produkten er beworben wird oder auf welchem Wege ihm Werbung zugehen soll. Das Kredit-Scoring hingegen wird zur Risikominimierung bei der Vergabe von Krediten verwendet: Soll ein Kredit an einen Verbraucher vergeben werden, so wird zuvor das konkrete Risiko eines Kreditausfalls bewertet. Außerdem kommen Scoring-

[337] Eine entsprechende Übersicht findet sich im [ULD-Scoring-Gutachten 2006, S. 12 ff.].
[338] Hierzu [ULD-Scoring-Gutachten 2006, S. 13].
[339] Ausführlich beleuchtet werden Fragestellungen des Verbraucher-Scorings von [Weichert 2006].

Verfahren zunehmend in solchen Bereichen zum Einsatz, in denen für die Unternehmensseite ein wirtschaftliches Risiko besteht, an dessen Bewertung sie ein vitales Interesse hat.[340] Konkret ist dies regelmäßig in solchen vertraglichen Konstellationen der Fall, in denen das Unternehmen gegenüber dem Verbraucher in Vorleistung tritt. Zu nennen sind hier neben dem Bereich der Versicherungswirtschaft auch die Wohnungs-, Kfz-Leasing- oder die Telekommunikationsbranche. Ebenfalls relevant ist das Scoring für den Versandhandel und den Online-Handel (E-Commerce) – hier geht es etwa um die Frage, ob eine Ware auf Rechnung oder nur gegen Vorkasse bzw. per Nachnahme erbracht wird.[341]

Nachfolgend wird am Beispiel des Kredit-Scorings dargestellt, welche Kundendaten bei einem Verbraucher-Scoring üblicherweise miteinander verkettet werden, auf welcher Rechtsgrundlage dies geschieht bzw. geschehen darf und wie es um die Transparenz eines solchen Scorings für den Verbraucher bestellt ist.[342]

3.3.4.2 Verbraucherkredit-Scoring

3.3.4.2.1 Allgemeines

Ziel des Kredit-Scorings ist es, eine Prognose zu einem konkreten Kreditausfallrisiko zu erstellen – es soll also vorhergesagt werden, mit welcher Wahrscheinlichkeit ein (potenzieller) Kreditnehmer einen eingeräumten Kredit zurückzahlen wird. Dieses Risiko wurde in früheren Jahren ausschließlich von einem Sachbearbeiter auf der Grundlage eines persönlichen Gesprächs bewertet. Diese subjektive Art der Entscheidungsfindung ist aber im Laufe der Zeit mehr und mehr durch die mathematisch-statistischen Verfahren des Scorings ergänzt bzw. verdrängt worden.[343] Dabei sollen Letztere insbesondere eine Verobjektivierung der Kreditvergabe ermöglichen.

Der Score-Wert ist im Übrigen häufig nicht nur für die Entscheidung, ob überhaupt ein Kredit gewährt wird, sondern auch für die Beantwortung der Frage, zu welchen Konditionen (insbesondere Zinssatz und Laufzeit) ein Kredit eingeräumt wird, von Bedeutung.[344]

Scoring-Verfahren können von dem jeweiligen Kreditinstitut selbst (*internes Scoring*) oder von dritten Stellen (*externes Scoring*) durchgeführt werden.[345] Bei solchen spezialisierten Scoring-Unternehmen handelt es sich um Auskunfteien und Konzern- oder Verbandsdienstleister. Auskunfteien erteilen in der Regel nicht nur Auskunft über die bei ihnen gespeicherten Positiv- und Negativmerkmale von Verbrauchern, sondern übermitteln auch Score-Werte zu dem jeweils angefragten Verbraucher. In Deutschland wird das professionelle externe Scoring von Organisationen wie der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA), der Informa Unternehmensberatung GmbH, der CED Creditreform Consumer GmbH und der Bürgel Wirtschaftsinformationen GmbH & Co. KG dominiert.[346]

3.3.4.2.2 Verkettete Informationen

Die Zahl der Merkmale, die in ein Kredit-Scoring einfließen, variiert von Verfahren zu Verfahren. Als Datenquellen kommen insoweit Angaben aus dem Vertragsantrag, Vertragsdaten aus unterschied-

[340] [Weichert 2006, S. 400].

[341] Außerdem sei an dieser Stelle auf das sog. Call-Center-Scoring hingewiesen. Hierbei werden zunächst verschiedene Kunden hinsichtlich ihrer Bedeutung bewertet und das Ergebnis dieser Bewertung mit der Telefonnummer des jeweiligen Kunden verknüpft. Rufen dann viele Kunden gleichzeitig bei dem Call-Center an, so richtet sich die Reihenfolge der Annahme der Anrufe nach der zuvor vorgenommenen Bewertung der anrufenden Telefonnummern bzw. der entsprechenden Kunden.

[342] Umfassend erörtert werden die hiermit verbundenen Fragestellungen im [ULD-Scoring-Gutachten 2006].

[343] [Weichert 2006, S. 400].

[344] [ULD-Scoring-Gutachten 2006, S. 19].

[345] Hierzu etwa [Abel 2006, S. 109].

[346] Ausführliche Informationen zu diesen spezialisierten Unternehmen finden sich im [ULD-Scoring-Gutachten 2006, S. 32 ff.].

lichen Vertragsverhältnissen zwischen dem Unternehmen und dem jeweiligen Verbraucher, soziodemographische Daten und Angaben von Auskunfteien in Betracht.[347]

Beim internen Scoring kommt es in zweifacher Hinsicht zu einer Merkmalsverkettung: Zum einen werden Daten aus früheren Konsumentenverträgen miteinander verkettet[348], um hieraus bestimmte Gesetzmäßigkeiten und generelle Prognosen abzuleiten, zum anderen werden einschlägige Merkmale des einen Kredit beantragenden Verbrauchers miteinander verkettet, um dann anhand dieser Datenbasis und der zuvor ermittelten Korrelationen eine Prognose für den konkreten Einzelfall zu treffen.

Beim externen Scoring werden vielfach noch wesentlich umfangreichere Verkettungen vorgenommen. So sei an dieser Stelle angemerkt, dass etwa die SCHUFA über einen Gesamtdatenbestand verfügt, in dem Daten zu ca. 59 Millionen Personen gespeichert sind.[349]

Im [ULD-Scoring-Gutachten 2006] werden beim Scoring drei unterschiedliche Merkmalsgruppen (sog. Bonitätskriterien) unterschieden[350]: Vertragsdaten, Angaben zu den allgemeinen finanziellen Verhältnissen und soziodemographische Daten. Die nachfolgende, entsprechend unterteilte Übersicht listet einige Merkmale auf, die für ein Scoring in Betracht kommen (siehe Tabelle 14):[351]

Vertragsdaten		
Einzeltransaktionen/Kontoumsätze	Kontensaldi/Überziehungen	Vertragsverläufe/Zahlungsmoral
Zahl der Konten	Zahl und Höhe der Kredite	Zahl der Kreditkarten
Angaben zu den allgemeinen finanziellen Verhältnissen		
Vermögen	Höhe der Verbindlichkeiten	(verfügbares) Monatseinkommen
monatliche Ausgaben	Art und Zahl der Kredite	Insolvenz
Soziodemographische Daten		
Adresse	Geschlecht	Familienstand und Zahl der Kinder
Alter	Beruf	Nationalität

Tabelle 14: Merkmale, die im Rahmen eines Scorings relevant sein können

3.3.4.2.3 Rechtliche Aspekte

Wie jede andere Verarbeitung personenbezogener Daten kann auch die Datenverarbeitung beim Scoring entweder durch die Einwilligung des Betroffenen nach § 4a BDSG oder durch eine gesetzliche Grundlage legitimiert werden.[352]

3.3.4.2.3.1 Einwilligung des Betroffenen

Die Durchführung eines Scorings kann aus datenschutzrechtlicher Sicht zum einen dann zulässig sein, wenn eine wirksame Einwilligung des betroffenen Verbrauchers vorliegt.[353] Diese muss zeitlich

[347] [ULD-Scoring-Gutachten 2006, S. 26].
[348] Ggf. werden diese Daten zusätzlich mit weiteren statistischen Informationen verkettet, die aus externen Quellen stammen. Darüber hinaus besteht auch die Möglichkeit, dass ein extern erstellter Score-Wert als ein Merkmal von vielen in die Berechnung eines internen Score-Werts einfließt und insoweit noch eine weitere Verkettung vorgenommen wird.
[349] [ULD-Scoring-Gutachten 2006, S. 50 ff.].
[350] [ULD-Scoring-Gutachten 2006, a.a.O.].
[351] Im Einzelnen vgl. [ULD-Scoring-Gutachten 2006, a.a.O.].
[352] Umfangreiche Ausführungen zur rechtlichen Zulässigkeit von Scoring-Verfahren finden sich im [ULD-Scoring-Gutachten 2006, S. 71 ff.] und bei [Abel 2006, S. 110 ff.].
[353] Ausführlich hierzu [ULD-Scoring-Gutachten 2006, S. 71].

vor der Score-Berechnung und in schriftlicher Form erteilt werden. Wegen der hohen Komplexität des Kredit-Scorings ist von besonderer Bedeutung, dass die Einwilligung hinsichtlich Zweck, verantwortlicher Stelle und verwendeter Daten bzw. durchgeführter Datenverarbeitung hinreichend bestimmt ist.[354] Sofern auch soziodemographische Daten für das Verfahren verwendet werden, muss dies ausdrücklich erwähnt werden, da mit einer Verarbeitung solcher Daten ein hohes Diskriminierungsrisiko verbunden ist.

Dem [ULD-Scoring-Gutachten 2006] zufolge werden ausdrückliche Einwilligungen ohne eine direkte Vertragsbindung im Scoring-Kontext gegenwärtig praktisch nicht eingeholt.

3.3.4.2.3.2 Gesetzliche Grundlage

Da also die Einwilligung des Betroffenen als Rechtsgrundlage für die Durchführung eines Scorings bisher in der Praxis kaum eine Rolle spielt, kommt es entscheidend darauf an, durch welche Rechtsvorschriften die Datenverarbeitung legitimiert werden kann. Insofern ist zunächst zu prüfen, ob hier spezielle gesetzliche Regelungen einschlägig sind.

Der Gesetzgeber hat im Zuge der Umsetzung der EU-Richtlinien zu Basel II in deutsches Recht erstmals bereichsspezifische Vorschriften zur Verwendung interner Risikomessverfahren und insbesondere von Ratingsystemen (= Scoring) geschaffen.[355] Diese finden sich in § 10 Abs. 1 S. 3-8 Kreditwesengesetz (KWG) und sind am 01. Januar 2007 Kraft getreten. Die genannte Vorschrift gilt nach Auffassung der Datenschutzaufsichtsbehörden als bankenaufsichtsrechtliche Norm allerdings nur für die Erhebung und Verarbeitung personenbezogener Daten zur internen Risikobemessung (Eigenkapitalausstattung), nicht jedoch für das Scoring im Außenverhältnis zu den (potenziellen) Kunden. Die neuen Vorschriften verdrängen daher die generellen Vorschriften des Bundesdatenschutzgesetzes nicht. Damit sind im Ergebnis primär die Regelungen des §§ 28 ff. BDSG einschlägig.

Bei einer Verarbeitung personenbezogener Daten im Rahmen von Scoring-Verfahren, die durch das jeweilige Kreditinstitut selbst durchgeführt werden (internes Scoring), werden hinsichtlich der Frage, welcher Tatbestand des § 28 BDSG insoweit anwendbar ist, unterschiedliche Ansichten vertreten:

Nach Auffassung der Datenschutzaufsichtsbehörden kommt als Rechtsgrundlage hierfür in erster Linie § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht.[356] Danach ist eine Verarbeitung personenbezogener Daten zulässig, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Datenverarbeitung überwiegt. Ob diese Voraussetzungen vorliegen, muss in jedem Einzelfall sorgfältig überprüft werden. Bei dieser Abwägung können die Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG berücksichtigt werden. Diese Ansicht der Datenschutzaufsichtsbehörden ist nach der hier vertretenen Auffassung allerdings noch dahingehend zu präzisieren, dass eine Berücksichtigung dieser Wertungen nur dann möglich ist, wenn die konkrete Regelung nicht zu Lasten des Verbrauchers geht, sondern die erlaubte Datenverarbeitung inhaltlich einschränkt. Die Merkmale müssen daher nicht nur mathematisch-statistisch erheblich sein, sondern eine ebenso hohe Stringenz aufweisen wie die im Merkmalskatalog des § 10 Abs. 1 Satz 6 KWG aufgeführten Regelbeispiele. Angaben wie z.B. solche zur Staatsangehörigkeit sind bereits aufgrund des ausdrücklichen Verbots in

[354] Bezüglich des Zwecks genügt es insoweit, wenn dieser mit „Prognose des Kreditrisikos“ benannt wird. Als Daten verarbeitende Stelle müssen das jeweilige Kreditinstitut und bei einem externen Scoring auch das Scoring-Unternehmen aufgeführt werden. Hinsichtlich der verarbeitenden Daten ist eine eindeutige Kategorisierung wie „die im Antrag genannten Daten“ ausreichend.

[355] Zur Kritik an diesen Vorschriften vgl. [Weichert 2006, S. 404]. Diese Ausführungen bezogen sich damals noch auf den entsprechenden Gesetzentwurf der Bundesregierung. Eine ausführliche Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zu diesem Gesetzentwurf findet sich zudem unter https://www.datenschutzzentrum.de/scoring/060404-bankenrichtlinie.htm (letzter Zugriff im Oktober 2007).

[356] Vgl. den Beschluss des sog. Düsseldorfer Kreises zu Kredit-Scoring / Basel II vom 19./20.04.2007, abrufbar unter http://www.bfdi.bund.de/cln_030/nn_531946/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DuesseldorferKreis/April07Basel2,templateId=raw,property=publicationFile.pdf/April07Basel2.pdf (letzter Zugriff im Oktober 2007).

§ 10 Abs. 1 Satz 3 KWG als Score-Merkmale ausgeschlossen. Bei der Abwägung ist darüber hinaus anhand von Wertungen des Grundgesetzes wie auch des einfachen Rechts zu überprüfen, ob eine Benachteiligung der (potenziellen) Kunden aufgrund eines bestimmten Kriteriums unzumutbar ist.

Nach der im [ULD-Scoring-Gutachten 2006] vertretenen Ansicht muss das Scoring hingegen zum Bestandteil des Kreditvertrages gemacht werden, so dass als Rechtfertigungsgrundlage § 28 Abs. 1 Satz 1 Nr. 1 BDSG in Betracht kommt. Für den Vertragszweck des Kreditvertrages sind dabei nur solche Scoring-Verfahren als dienlich anzuerkennen, mit deren Hilfe auch tatsächlich valide Aussagen zur Kreditwürdigkeit und Ausfallwahrscheinlichkeit eines Verbrauchers getroffen werden können[357], d.h., die eine konkrete Relevanz für das vorherzusagende Verhalten besitzen. Insoweit ist auch die Zulässigkeit der einzelnen für das Scoring verwendeten Merkmale zu prüfen. Diese müssen eine wissenschaftlich-statistische Relevanz besitzen und korrekt gewichtet sein. Außerdem müssen die gewonnenen Erkenntnisse plausibel nachvollzogen werden können und schließlich ist sicherzustellen, dass der Nutzung der Merkmale keine Nutzungsverbote entgegenstehen. So dürfen etwa besonders sensitive personenbezogene Daten – z.B. zur Gesundheit einer Person – im Rahmen eines Scorings nur dann verwendet werden, wenn der Verbraucher hierzu seine Einwilligung erteilt.[358]

Wird ein externes Scoring durchgeführt, so ist darüber hinaus auch noch zu prüfen, ob auch die Übermittlung an das spezialisierte Drittunternehmen und die dort erfolgende Datenverarbeitung auf eine gesetzliche Grundlage gestützt werden können.[359]

3.3.4.2.3.3 Verbot der automatisierten Einzelentscheidung

Bei der Durchführung eines Kredit-Scorings muss weiterhin die Vorschrift des § 6a Abs. 1 BDSG berücksichtigt werden, wonach Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden dürfen, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Hierdurch soll sichergestellt werden, dass für den Betroffenen nachteilige Entscheidungen nicht ausschließlich automatisiert getroffen werden, sondern dass hier stets noch eine Überprüfung durch einen Menschen vorgenommen wird. Konkret soll also beim Scoring ausgeschlossen werden, dass der Score-Wert als alleinige Entscheidungsgrundlage für die (Nicht-)Vergabe eines Kredits dient.

3.3.4.2.4 Transparenz

Aufgrund der hohen Komplexität von Scoring-Verfahren sind besonders hohe Anforderungen an deren Transparenz zu stellen. Der Verbraucher muss vor der Durchführung eines Scorings informiert werden[360] über:

- Zweck und Durchführung des Scorings,
- die Identität des das Scoring durchführenden Kreditinstituts,
- über die Tatsache der Durchführung eines externen Scorings,
- die im Rahmen des Scorings ausgewerteten Merkmale sowie
- die Einbeziehung soziodemographischer Daten.

Zudem hat der von einem Scoring betroffene Verbraucher einen Anspruch auf Auskunft über seinen Score-Wert und dessen Bedeutung. Bei diesem handelt es sich nämlich um ein personenbezogenes Datum, das nach § 34 BDSG beauskunftet werden muss.[361] Nach Ansicht der Datenschutzaufsichtsbehörden[362] muss dem Betroffenen insoweit auch Auskunft zu den vier für das Ergebnis des Scorings

[357] [Weichert 2006, S. 401].
[358] Dies ergibt sich aus § 28 Abs. 6 BDSG, da die dort aufgeführten sonstigen Erlaubnistatbestände beim Scoring in aller Regel nicht einschlägig sein dürften.
[359] Auf Einzelheiten kann an dieser Stelle nicht eingegangen werden, Ausführungen hierzu finden sich etwa bei [Weichert 2006, S. 401] und bei [Abel 2006, S. 111].
[360] Die Verpflichtung hierzu kann sich aus §§ 4a Abs. 1 S. 2, 4 Abs. 3 oder 33 Abs. 1 S. 1 BDSG ergeben.
[361] H. M. Vgl. nur [Gola/Schomerus 2005, § 3 Rn. 3] und [Abel 2006, S. 110 m.w.N.].
[362] Dieselbe Ansicht wird auch im [ULD-Scoring-Gutachten 2006] vertreten.

wichtigsten Merkmalen erteilt werden, die dann in der Reihenfolge ihrer Bedeutung aufzuführen sind. Wird die Beauskunftung in der Praxis teilweise von der Zahlung eines Entgelts abhängig gemacht, so widerspricht dies im Übrigen der vorgenannten Vorschrift, nach deren Abs. 5 Auskünfte unentgeltlich erteilt werden müssen.

Auch wenn das Gesetz klare Anforderungen an die Information und Beauskunftung des – von einem Scoring – betroffenen Verbrauchers stellt, ist die Transparenz von Scoring-Verfahren in der Praxis vielfach defizitär. Der Verbraucher weiß in der Regel nicht, welche Daten in ein Scoring einfließen und mittels welcher Kriterien diese ausgewertet werden. In vielen Fällen wird er noch nicht einmal darüber informiert, dass überhaupt ein Scoring stattfindet.[363]

3.3.4.3 Fazit

Bei der Durchführung von Scoring-Verfahren wird eine Vielzahl von Merkmalen der betroffenen Verbraucher verkettet und mit Hilfe unterschiedlicher Verfahren ausgewertet. Dabei kann ein negativer Score-Wert dazu führen, dass dem betroffenen Verbraucher die Einräumung eines Kredits ganz verweigert wird. Darüber hinaus kann sich der Score-Wert auch auf die Konditionen eines Kreditvertrags wie etwa Zinshöhe oder Laufzeit auswirken. Selbst wenn ein Verbraucher der Durchführung eines Scorings bzw. der Übermittlung eines Score-Werts durch eine Auskunftei widerspricht, kann sich dies nachteilig auswirken, wenn die Bank daraufhin einen Vertragsschluss ablehnt. Scoring-Verfahren können für die hiervon betroffenen Personen also drastische wirtschaftliche Auswirkungen haben. Äußerst kritisch zu bewerten ist deshalb der Umstand, dass in der Praxis das gesetzlich vorgeschriebene Maß an Transparenz oft nicht eingehalten wird, obwohl dies für den Verbraucher gerade in diesem Kontext besonders wichtig wäre.

3.3.5 Kundenbindungssysteme

3.3.5.1 Einleitung

Mit der Kundenkarte können die Kunden ihre Einkäufe registrieren lassen und werden für diese „Treue“ zumeist durch Rabatte in verschiedenen Formen belohnt. Die Rabattansprüche werden in der Regel erfasst, indem eine mit einem Magnetstreifen oder einem Chip versehene Karte beim Kauf vom Kunden vorgezeigt werden muss. Die Karte enthält darauf identifizierende Daten über den Teilnehmer am Kundenbindungssystem.

Die eingesetzten Kundenbindungssysteme[364] lassen sich im Wesentlichen in zwei verschiedene Grundformen einteilen. Zum Teil werden Kundenkarten von den Unternehmen an ihre eigenen Kunden ausgegeben, um diese mit Vergünstigungen und besonderen Serviceleistungen an das Unternehmen zu binden. Zum Teil werden die Kundenbindungssysteme unternehmensübergreifend ausgestaltet. Letztere Systeme werden von einem zentralen Systemverwalter verwaltet und sind darauf angelegt durch die Vereinigung mehrere Branchen einen weitreichenden Konsumbereich der Kunden der teilnehmenden Unternehmen abzudecken. Die Kundenkarte kann zu diesem Zweck unternehmensübergreifend bei allen teilnehmenden Partnerunternehmen eingesetzt werden. Für Fragen der Verkettung sind gerade die Kundenbindungssysteme in einem solchen Mehr-Parteien-Verhältnis von besonderem Interesse. Abbildung 5 verdeutlicht die Beziehungen in einem Mehr-Parteien-Verhältnis.

[363] [ULD-Scoring-Gutachten 2006, S. 44].
[364] Ausführlich zu Kundenbindungssystemen und Datenschutz [ULD-Kundenbindungsstudie 2003].

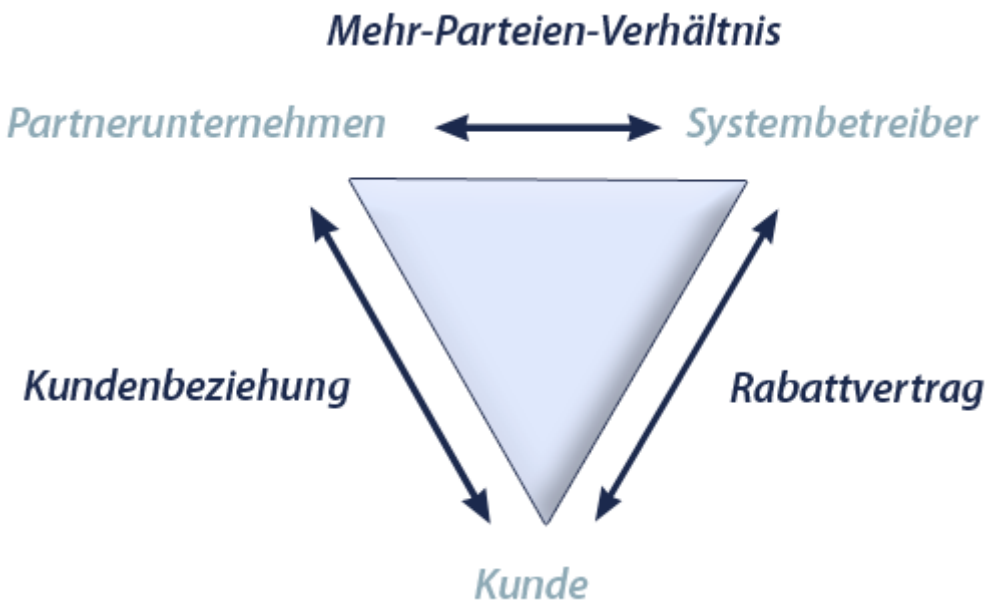


Abbildung 5: Mehr-Parteien-Kundenbindungssystem

Aus Unternehmenssicht werden Kundenbindungssysteme betrieben, um gezielte Werbung und Marktforschung betreiben zu können. Je detaillierter dabei die Informationen über die Vorlieben und die finanzielle Situation des Kunden sind, desto genauer kann der Unternehmer seine Werbeansprache steuern, um dadurch die Effektivität seiner Absatzbemühungen steigern.

3.3.5.2 Anfallende Datenkategorien

Bei den im Rahmen von Kundenbindungssystemen erhobenen bzw. anfallenden Daten ist zu unterscheiden zwischen Stammdaten, Programmdaten und sonstigen Angaben.

Unter Stammdaten sind die Identifikations- bzw. Kontaktinformationen wie Name, Anschrift, Geburtsjahr und Telefonnummer zu verstehen. Diese Angaben werden zumeist über das Anmeldeformular bei Vertragsschluss erfragt und sind dort in der Regel als Pflichtangaben des Kunden gekennzeichnet.

Die Programmdaten fallen beim Einkauf mit der Kundenkarte an. Setzt der Kunde seine Karte bei einem Einkauf oder bei der Inanspruchnahme einer Dienstleistung ein, wird dort eine Reihe von Daten über diesen Vorgang festgehalten. Dabei handelt es sich gewöhnlich um eine Kennung des Kunden, etwa durch eine Kunden- oder Kartennummer, die Kennung des beteiligten Partnerunternehmen bei Kundenbindungssysteme im Mehr-Parteien-Verhältnis, Ort, Datum und Uhrzeit des Karteneinsatzes, den Umsatz sowie u.U. auch Angaben über die erworbene Ware oder die in Anspruch genommene Dienstleistung nach Waren- oder Dienstleistungsgruppen. Die Partnerunternehmen übermitteln diese Programmdaten jeweils bei einem Einkauf und übermitteln sie dann an den Systembetreiber.

Über das Anmeldeformular werden häufig noch weitere Daten der Kunden erhoben. Hierbei handelt es sich etwa um Angaben zum Familienstand, Haushaltsgröße und -einkommen, Hobbys oder Konsumvorlieben.

In der Regel werden neben den Programmdaten zur Rabattgewährung auch die Kundendaten beim Systembetreiber gespeichert. Während der Systembetreiber Kenntnis dieser Stammdaten für die Rabattverwaltung benötigt, besteht auf Seiten der Partnerunternehmen Interesse an den Stammdaten, um Werbemaßnahmen durchführen zu können. Den Partnerunternehmen wird vom Systembetreiber entweder die Möglichkeit der Nutzung der Stammdaten auch für eigene Zwecke eingeräumt oder die Daten werden sogar an diese übermittelt.[365]

[365] [ULD-Kundenbindungsstudie 2003, S. 30].

3.3.5.3 Rechtsgrundlagen

Als Rechtsgrundlagen für die Verarbeitungen dieser Daten kommen die gesetzlichen Tatbestände des § 28 BDSG sowie die Einwilligung des Betroffenen nach § 4a BDSG in Betracht. Wichtig ist in diesem Zusammenhang zu unterscheiden, zu welchen Zwecken welche Daten von welchen Beteiligten verarbeitet werden. Die Verarbeitung von Stammdaten und Programmdaten ist in der Regel notwendig, um den Rabattvertrag durchzuführen und abzuwickeln, so dass sich die Verarbeitung auf § 28 Abs. 1 BDSG stützen lässt. Ausnahmen können aber in Bezug auf die Erfassung des vollständigen Geburtsdatums bzw. die Kenntnis der Warengruppen bzw. der konkreten Produkte bestehen. In der Regel wird die Verarbeitung dieser Informationen für die Durchführung der Rabattgewährung nicht erforderlich sein.

Für die zweckändernde Nutzung der Daten zu Werbe- und Marktforschungszwecken muss, soweit dabei Daten jenseits von Name, Adresse und Geburtsjahr bzw. Berufsbezeichnung verwendet werden, in der Regel eine Einwilligung der Kunden vorliegen. Bei der Verwendung der Daten für Zwecke der Werbung und Marktforschung durch den Systembetreiber im Rahmen von Kundenbindungssystemen im Mehr-Parteien-Verhältnis dürfen die Daten nur mit Einwilligung des Betroffenen verarbeitet werden. Eine gesetzliche Rechtfertigungsgrundlage scheidet aus, da hier regelmäßig schutzwürdige Interessen der Kunden entgegenstehen.

3.3.5.4 Verkettbarkeit

Möglichkeiten der Verkettung ergeben sich insbesondere für die Systeme im Mehr-Parteien-Verhältnis. Hier laufen beim Systembetreiber Daten der Kunden aus unterschiedlichsten Konsumbereichen auf, die miteinander verknüpft werden können. Über die Kennung des Kunden, die Kunden- oder Kartennummer, wird eine Zuordnung der Daten zu bestimmten Personen vorgenommen. Dabei lassen die anfallenden Programmdaten Rückschlüsse über Lebensgewohnheiten des Teilnehmers zu. Über den Ort und die Zeit des Umsatzes in Verbindung mit dem Stammdatum Anschrift lassen sich beispielsweise in Zusammenschau mit Benzinverbrauch und Nutzung von Telefonverbindungen Erkenntnisse über Verhaltensmuster und zudem den üblichen Aufenthaltsort des Kunden zu. Dies gilt umso mehr, je häufiger der Kunde seine Karte einsetzt.

Zudem besteht die Möglichkeit, diese Informationen z.B. mit externen Bonitätsinformationen anzureichern bzw. über statistische Auswertungen der in großem Umfang vorliegenden Konsumdaten zusätzliche Erkenntnisse zu generieren.

Immer größere Bedeutung kann durch Ausweitung der bestehenden Eingriffsgrundlagen für Polizei und Verfassungsschutz einem Zugriff durch Ermittlungsbehörden auf Datenbestände der Privatwirtschaft zukommen, die im Einzelfall einen umfassendes Persönlichkeitsprofil bereithalten können.

3.3.5.5 Transparenz

Die Möglichkeit, aus den je nach Häufigkeit des Karteneinsatzes umfangreichen Programmdaten ein Kundenprofil zu erstellen, ergibt sich für die Kunden des Kundenbindungssystems aus den Allgemeinen Geschäftsbedingungen sowie den Datenschutzerklärungen der Systembetreiber. Bekannte Mehr-Parteien-Kundenbindungssysteme in Deutschland sind beispielsweise Miles & More, Payback und Happy Digits. In den Teilnahmebedingungen[366] von Miles & More heißt es dabei etwa: „zu Werbezwecken erfolgt auch eine Datenübermittlung an Partnerunternehmen und andere Dritte in dem Umfang, in dem der Teilnehmer bei seiner Anmeldung zu Miles & More eingewilligt hat.“ Die Datenschutzerklärung präzisiert den Verarbeitungszweck dahingehend, dass „maßgeschneiderte Angebote rund um das Miles & More Programm“ unterbreitet werden sollen[367]. Dem Kunden wird mitgeteilt, dass auf die speziellen Präferenzen des Kunden zugeschnittene Angebote unterbreitet werden sollen.

[366] Teilnahmebedingungen, Stand 23.07.2007. Abrufbar unter http://www.miles-and-more.com/online/portal/mam/de/programm/how_it_works?tl=1&l=de (letzter Zugriff im Oktober 2007).

[367] Datenschutzerklärung von Miles & More, Stand 23.07.2007. Abrufbar unter http://www.miles-and-more.com/online/portal/mam/de/nonav/generalinfo/privacy_statement?l=de (letzter Zugriff im Oktober 2007).

Beim Zusammenschluss vieler Partnerunternehmen aus unterschiedlichen Branchen ist der hinter dem System stehende Betreiber für den Kunden als zentrale Stelle, bei der die verschiedenen Konsumdaten zusammengeführt werden, in der Regel nicht wie das Partnerunternehmen, bei dem ein Einkauf getätigt wird, ohne weiteres erkennbar. Welche Daten der Systembetreiber zusammengeführt hat und welche davon zur Profilbildung genutzt werden, weiß der Kunde nicht. Ist eine Profilbildung beabsichtigt, muss darauf bei der Einholung einer Einwilligung deutlich hingewiesen werden [ULD-Kundenbindungsstudie 2003].

Dem Kunden steht als Betroffenem der Auskunftsanspruch aus § 34 BDSG zur Seite. Er kann Auskunft über sämtliche zu seiner Person gespeicherten Daten verlangen. Dies sind seine Stammdaten, seine freiwilligen Angaben und die Programmdaten.

Eine besondere Verringerung der Transparenz eines Kundenbindungssystems für den Kunden kann sich durch den Einsatz von RFID im Rahmen des Systems ergeben. Payback hatte testweise Kundenkarten mit RFID-Chips versehen und dabei für Unmut von Verbraucherschützern gesorgt.[368] Denn dabei hatte das Unternehmen sowohl versäumt, die Karteninhaber über die eingebauten Tags zu informieren, als auch eine notwendige Einwilligung einzuholen. Technisch erlaubt RFID das kontaktlose Auslesen der auf dem RFID-Chip gespeicherten Informationen. Dies ist in der Regel immer mindestens eine Identifikationsnummer, über die sich der Karteninhaber identifizieren lässt, ohne sich dessen bewusst zu sein oder sich etwa für einen Karteneinsatz entschieden zu haben. Neben der Information, wer zu welchem Zeitpunkt welche Produkte gekauft hat, lässt sich über den Einsatz von RFID in der Kundenkarte auch erfassen, wie lange ein Kunde vor welchem Regal und insgesamt im Laden verbracht hat.

Üblicherweise kommuniziert das Lesegerät mit jedem RFID-Chip, und dies geschieht, ohne dass die Datenübermittlung für den Betroffenen wahrnehmbar ist. Angesichts des hohen Aussagewerts der zentral beim Systembetreiber zusammengeführten Programmdaten verringert der Einsatz von RFID in Kundenbindungssystemen die Kontrollierbarkeit der Datengewinnung und -nutzung für den Kunden empfindlich stark.

3.3.6 Suchmaschinen: Verkettung von Suchanfragen

3.3.6.1 Einleitung

Für die Nutzung des Internets dienen Suchmaschinen wie Yahoo, Google oder AOLSearch[369] dem Nutzer zum Auffinden von Inhalten über Suchanfragen. Eine Suchanfrage ist dabei ein einzelner oder eine Aneinanderreihung von Suchbegriffen, auf die die jeweilige Suchmaschine eine Liste von Internetseiten mit ihrer jeweiligen Internetadresse zurückliefert. Je nach Nutzungsverhalten geben die Suchanfragen in vielfältiger Weise Aufschluss über die Gewohnheiten, Interessen und Tätigkeiten eines Nutzers.

AOL veröffentlichte im August 2006 einen Auszug von Suchanfragen von über 500.000 Nutzern ihrer Suchmaschine zu Forschungszwecken.[370] Dabei waren die Nutzernamen durch Zahlen ersetzt, die einen Rückschluss auf die dahinter stehenden Personen verhindern sollten. Einige der Suchanfragen wiesen allerdings eindeutige Hinweise auf ihren Verfasser auf, so dass in diesen Fällen Rückschlüsse auf einzelne Personen möglich waren. Diese Veröffentlichung verdeutlichte ein weiteres Mal die Sensibilität derartiger Datenbestände. AOL löschte nach massiver Kritik von Nutzern und Bürgerrechtsorganisationen den Datenbestand zwar wieder aus dem Netz[371]; er ist allerdings nach wie vor im Internet verfügbar (siehe Abbildung 6).[372]

[368] Telepolis vom 20.02.2004: „RFID-Chips in Metro-Payback-Kundenkarten versteckt“. Abrufbar unter http://www.heise.de/tp/r4/artikel/16/16803/1.html (letzter Zugriff im Oktober 2007).

[369] Daneben existiert eine Vielzahl anderer Suchdienste im Internet, deren Behandlung jedoch den Rahmen der vorliegenden Arbeit sprengen würde.

[370] http://www.heise.de/newsticker/meldung/76474/ (letzter Zugriff im Oktober 2007).

[371] http://www.eff.org/Privacy/AOL/spreadtheword.php (letzter Zugriff im Oktober 2007).

[372] http://www.aolsearchdatabase.com/ (letzter Zugriff im Oktober 2007).

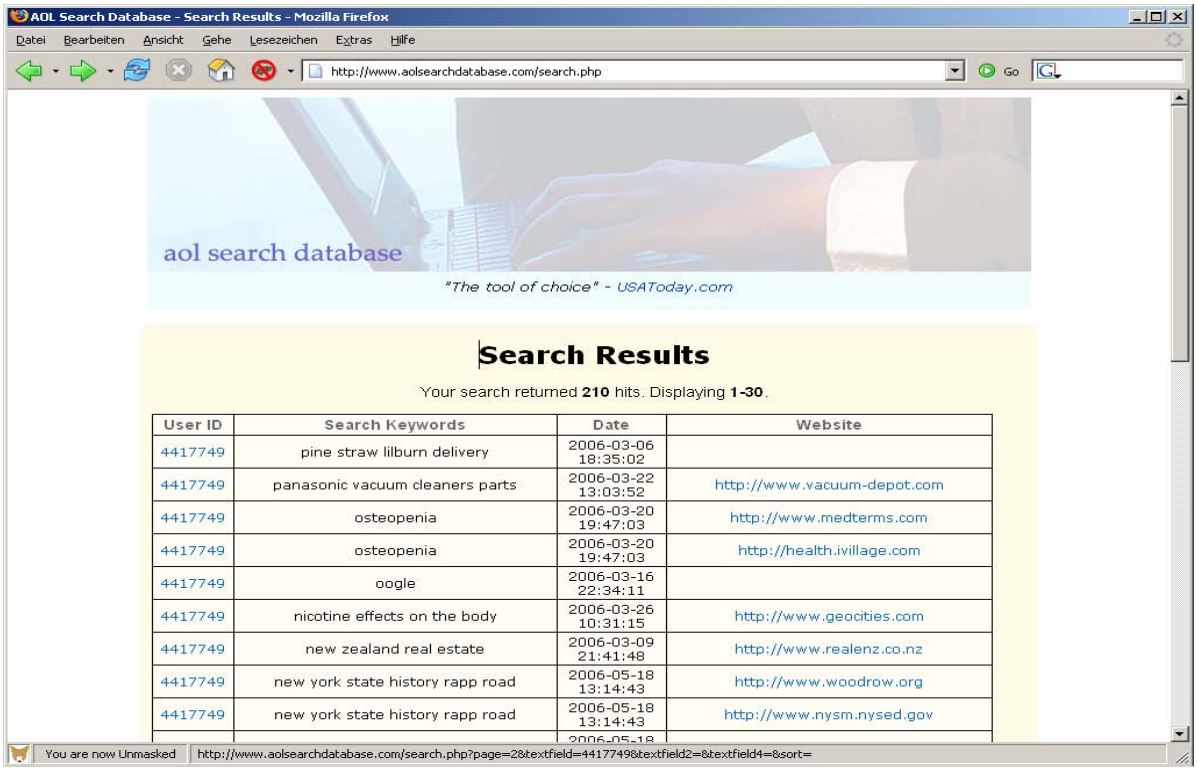


Abbildung 6: Screenshot: AOLsearchdatabase.com

3.3.6.2 Beim Suchmaschinenbetreiber anfallende Daten

Bei einem Suchvorgang fallen beim Betreiber der Suchmaschine zumeist[373] folgende Daten an (siehe Tabelle 15):

Daten der eigentlichen Suche	
Suchanfrage (ein oder mehrere Suchbegriff(e))	Datum und Uhrzeit der Anfrage
Technisch bedingt übertragene Daten (sog. „Browser-Chatter“)	
IP-Adresse des anfragenden Computers	ggf. der Inhalt eines Cookies[374]
benutzter Browser und Betriebssystem	weitere Angaben eines HTTP-Requests[375]
die vom Nutzer ausgewählte Internetseite	ggf. weitere Daten

Tabelle 15: Anlässlich eines Suchvorgangs beim Suchmaschinenbetreiber anfallende Daten

[373] Der genaue Datenbestand variiert von Suchmaschine zu Suchmaschine. So speichert AOL neben der ausgewählten Internetseite auch deren Position in der Reihenfolge der gefundenen Internetseiten.

[374] Ein Cookie kann im Browser deaktiviert werden. Teilweise werden neben Cookies auch andere Techniken eingesetzt, vgl. http://www.google.com/intl/en/privacy.html (letzter Zugriff im Oktober 2007).

[375] Vgl. RFC 2616.

3.3.6.3 Technische Realisierung einer Verkettung von Suchanfragen

3.3.6.3.1 Über die IP-Adresse

Die Verkettung der Suchanfragen untereinander, aber auch mit anderen Daten kann bei Suchmaschinen insbesondere über die IP-Adresse erfolgen, die den abfragenden Computer ausweist. Durch den Einsatz von Anonymisierungs-Proxies[376] und dynamischen IP-Adressen weisen diese Ergebnisse jedoch für den Betreiber Verfälschungen und Ungenauigkeiten auf.

3.3.6.3.2 Über Cookies

Daher wird oftmals der Einsatz von Cookies vorgezogen, die einen Computer, bzw. einen Browser auch dann noch eindeutig identifizieren, wenn die IP-Adresse zwischenzeitlich geändert wurde. Cookies werden oft auch im Interesse des Nutzers verwendet, um ihn beispielsweise für die Nutzung personalisierter Dienste[377] wiederzuerkennen und so den Aufwand einer erneuten Anmeldung zu ersparen.

3.3.6.4 Umgang mit dem Datenbestand

Der Umgang der Suchmaschinenbetreiber mit den von ihnen gesammelten Daten ist uneinheitlich. So speichert AOL den Datenbestand nur für einen Zeitraum von dreißig Tagen[378], während Google derzeit unbefristet speichert.[379]

Allen Anbietern dienen die gespeicherten Anfragen zunächst zur Optimierung der Leistung ihrer Suchmaschine; gleichzeitig werden sie aber oftmals auch eingesetzt, um zielgerichtete Werbung zu platzieren. Auch eine Weitergabe der Daten an Dritte zu Marktforschungszwecken ist nicht unüblich.[380]

Yahoo verwendet die entstandenen Daten ebenfalls zu Werbe- und Marktforschungszwecken sowie zur Verbesserung ihres Dienstleistungsangebotes. In der Datenschutzerklärung wird jedoch darauf hingewiesen, dass die Verwendung dadurch ausgeschlossen werden kann, dass im Browser die Nutzung von Cookies deaktiviert wird.[381]

3.3.6.5 Rechtmäßigkeit der Speicherung von Suchanfragen

In Deutschland und Europa unterliegt die Speicherung von personenbezogenen Daten den rechtlichen Bestimmungen des Datenschutzrechts.

---

376 So z.B. das Tor-Netz, http://tor.eff.org/ (letzter Zugriff im Oktober 2007).

377 Schon die Suchanfrage selber kann einen solchen personalisierten Dienst darstellen.

378 So zumindest http://www.eff.org/deeplinks/archives/005162.php (letzter Zugriff im Oktober 2007). In Deutschland werden nach http://www.aol.de/Portalkontakt-Datenschutz/lange-speichert-AOL-meine-Daten-1255476409-7.html (letzter Zugriff im Oktober 2007) Nutzungsdaten gelöscht oder anonymisiert, sofern sie nicht für Abrechnungszwecke benötigt werden.

379 Google hat kürzlich in einer Presseerklärung mitgeteilt sind, dass sie nach einer Intervention des Norwegischen Datenschutzbeauftragten von dieser Praxis abzuweisen beabsichtigen und nach einem Zeitraum von 18 bis 24 Monaten die Daten nur noch in anonymisierter Form speichern wollen (http://www.eff.org/deeplinks/archives/005162.php (letzter Zugriff im Oktober 2007)).

380 Vgl. etwa http://about.aol.com/aolnetwork/mem_commitments/ (letzter Zugriff im Oktober 2007). In der deutschsprachigen Datenschutzerklärung wird jedoch darauf hingewiesen, dass die Daten nur in anonymisierter Form oder mit ausdrücklicher Einwilligung weitergegeben werden – http://www.aol.de/Portalkontakt-Datenschutz/Welche-Daten-erhebt-AOL-AOL-Kunden-Zweck-1255476409-3.html (letzter Zugriff im Oktober 2007).

381 http://privacy.yahoo.com/privacy/de/ (letzter Zugriff im Oktober 2007). Ob diese Lösung rechtlichen Anforderungen gerecht wird, sofern nur auf diesem Wege dem Koppelungsverbot gem § 12 Abs. 3 TMG entgegen getreten werden soll, ist zweifelhaft.

3.3.6.5.1 Anwendbares Recht

Allerdings ist fraglich, ob überhaupt deutsches Datenschutzrecht anwendbar ist, da die meisten Suchmaschinenbetreiber ihre Dienste in einer Vielzahl von Ländern anbieten und ihren Sitz nicht immer in Deutschland haben. Nach § 1 Abs. 5 Satz 2 BDSG finden datenschutzrechtliche Vorgaben auch dann Anwendung, wenn die verantwortliche Stelle nicht in einem Mitgliedsstaat der EU belegen ist, sofern die Daten im Inland „erhoben, verarbeitet oder genutzt" werden. Suchmaschinen eröffnen dem Nutzer typischerweise die Möglichkeit, Suchanfragen über ein so genanntes Web-Formular an den Server des Betreibers zu versenden, wobei sich der Server nicht zwingend in Deutschland befinden wird.

Ob bei Nutzung von Eingabeformularen im WWW eine Erhebung im Inland vorliegt, wird in der Rechtswissenschaft uneinheitlich beantwortet.

3.3.6.5.1.1 Server-Standort

Dammann in [Simitis 2006, § 1 Rn. 219] will auf den Standort des Servers abstellen, da der Internetanbieter „keine Vorstellung davon hat, wer von dem Internetangebot Gebrauch machen wird. Es fehle ihm insoweit an einem konkretisierenden Erhebungswillen. Somit finde das BDSG nur dann Anwendung, wenn der Server im Inland stehen würde."

3.3.6.5.1.2 Client-Standort

Demgegenüber vertritt Scheja die Auffassung, dass für die Anwendbarkeit des BDSG der Standort des Clients maßgeblich sei [Scheja 2005]. Er kritisiert, dass Dammann mit seiner Auffassung eine Umgehung des BDSG ermögliche, da sich der Betreiber der Anwendung des BDSG entziehen könne, indem er den Server nicht in Deutschland aufstelle. Es könne so zu einer schlicht ungerechtfertigten Diskriminierung von Anbietern kommen, die im EU-Inland ihren Server betrieben und damit dem BDSG unterworfen seien, während andere, die unter Umständen auf den gleichen Markt abzielten, diese Anforderungen nicht zu erfüllen hätten.

Auch gehe Dammann nicht von den zutreffenden sachlichen Gegebenheiten aus. Art und Inhalt der einzugebenden Daten würden nämlich vom Betreiber des Internetangebotes vorgegeben. Zudem sei die Behauptung unzutreffend, dass der Internetanbieter keine Vorstellung davon habe, wer von seinem Angebot Gebrauch machen werde. So sei durch Wahl der „First-Level-Domain" sowie durch Sprachenwahl durchaus feststellbar, an wen sich das Angebot richte. Es fehle dem Anbieter auch nicht an einem konkreten Erhebungswillen, denn die Aufforderung an den Nutzer, im Rahmen eines Internetangebotes bestimmte Eingaben zu machen, basiere gerade auf einem konkreten Erhebungswillen [Scheja 2005, S. 90 f.].

3.3.6.5.1.3 Adressatentheorie

Im Ergebnis ist [Scheja 2005] wohl in den meisten Fällen recht zu geben. In Erwägungsgrund 20 der der Norm zugrundeliegenden EU-Datenschutzrichtlinie 1995/46/EG[382] heißt es: Es sind „Vorkehrungen zu treffen, um sicherzustellen, dass die in dieser Richtlinie vorgesehenen Rechte und Pflichten tatsächlich eingehalten werden". Es „ist zu vermeiden, dass einer Person der gemäß dieser Richtlinie gewährleistete Schutz vorenthalten wird."

Für die Erreichung dieses Ziels ist es unerheblich, in wessen Eigentum das „Mittel der Erhebung" steht. Vielmehr übt der Betreiber ab dem Augenblick, ab dem sich ein Nutzer für einen Service entschieden hat, die Kontrolle über die Nutzung aus, auch wenn dies auf dem Gerät des Nutzers, dem Client, geschieht. Grundsätzlich ist also unabhängig vom Standort des Servers BDSG anwendbar.[383]

Vieles spricht jedoch dafür, ein Adressatenelement zur Interpretation der Norm heranzuziehen (wie dies argumentativ, obgleich mit anderem Ergebnis, auch Dammann tut), um nicht uferlos zu werden.

[382] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zu Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[383] So wohl auch Art. 29-Datenschutzgruppe, Opinion 56 vom 20.05.2002, S. 10.

Es wäre wohl auch unbillig, solche Dienste dem deutschen Datenschutzrecht zu unterwerfen, die sich explizit an andere Rechtskreise richten.

Für jene Anbieter, die sich gezielt mit ihrem Angebot an Nutzer auch in Deutschland richten (und auch von deren Nutzung profitieren wollen), erscheint es zumutbar, dem BDSG unterworfen zu sein. Diese Interpretation ist schon allein deswegen erforderlich, um das beim Nutzer erzeugte Vertrauen in die Nutzung eines an ihn gerichteten Angebotes herzustellen und zu erhalten.

3.3.6.5.1.4 Anwendung der Adressatentheorie

Die Angebote der hier genannten Suchmaschinen richten sich sämtlich zumindest auch explizit an Nutzer in Deutschland. Sie weisen alle ein sprachlich lokalisiertes Angebot auf und sind unter Domains mit deutscher Länderkennung („.de“) zu erreichen. Insbesondere leitet Google sogar solche Anfragen, die unter ihrer www.google.com-Adresse von einem Client mit einer deutschen IP-Adresse eingehen, auf die .de-Adresse weiter[384]. Darüber hinaus wird eine Suche auf deutschsprachigen Webseiten und Webseiten in Deutschland als Option angeführt. Damit richten sich die Anbieter der bezeichneten Suchmaschinen ausdrücklich (auch) an deutsche Nutzer.

Das deutsche Datenschutzrecht ist somit auf die Speicherung von Suchanfragen der bezeichneten Suchmaschinenbetreiber örtlich anwendbar, vorausgesetzt, dass diese Suchanfragen von einem Client in Deutschland aus getätigt werden.

3.3.6.5.2 Erörterung der Rechtsgrundlagen

3.3.6.5.2.1 Einwilligung

Nach § 12 Abs. 1 TMG darf ein Diensteanbieter personenbezogene Daten nur erheben, sofern ihm dies gesetzlich gestattet ist oder der Nutzer eingewilligt hat. Eine Einwilligung kommt als Rechtsgrundlage allerdings nicht in Betracht. Für die Einwilligung gelten dieselben Bedingungen wie für eine nach § 4a BDSG[385], der nach allgemeiner Ansicht eine vorherige Einverständniserklärung in die Erhebung der personenbezogenen Daten vorsieht.[386] Eine solche Einverständniserklärung wird jedoch vor der Nutzung der bezeichneten Suchmaschinen nicht verlangt und nicht abgegeben.

3.3.6.5.2.2 Nutzungsdaten gem. § 15 Abs. 1 TMG

Eine Erhebung personenbezogener Daten ist allerdings nach § 15 Abs. 1 TMG zulässig, soweit dies für die Inanspruchnahme des Teledienstes erforderlich ist. Diese Norm stellt eine Rechtsgrundlage für eine vorübergehende Speicherung der Suchanfrage sowie der IP-Adresse des Nutzers dar, denn diese Angaben sind zur Bearbeitung der Anfrage erforderlich. Für eine Speicherung über die Bearbeitung hinaus sowie für die oben bezeichneten weiteren Daten wie etwa Zeitstempel oder Angaben über den Browser stellt die Norm keine Rechtsgrundlage dar.

3.3.6.5.2.3 Nutzungsdaten gem. § 15 Abs. 3 TMG

Allerdings räumt Abs. 3 dem Diensteanbieter die Speicherung für Zwecke der Werbung und Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien die Erstellung von Nutzungsprofilen ein. Hierin könnte eine Rechtsgrundlage für die Speicherung zu sehen sein.

Dabei muss der Diensteanbieter Pseudonyme verwenden. Außerdem schreibt die Norm vor, dass der Diensteanbieter ein Widerspruchsrecht anbieten und auf dieses hinweisen muss.

---

[384] http://www.heise.de/tp/r4/artikel/12/12948/1.html (letzter Zugriff im Oktober 2007).

[385] Gounalakis in Nomos-Erläuterungen zum deutschen Bundesrecht für den wortgleich ins TMG überführten § 3 TDDSG bei beck-online.

[386] [Gola/Schomerus 2005, § 4 Rn. 15].

In den Datenschutzerklärungen weisen die bezeichneten Anbieter darauf hin, dass die Verwendung von Cookies im Browser deaktiviert werden können, wobei das allerdings dazu führen könne, dass manche Elemente oder Dienste nicht richtig funktionieren.[387]

Ob diese Angaben hinreichend sind, um den Anforderungen des §15 Abs. 3 TMG genüge zu tun, ist zweifelhaft. Zwar könnte die über zwei Links erreichbare Datenschutzerklärung dem Erfordernis der Unterrichtung genügen. Die Deaktivierung der Cookies jedoch kann noch keine Ausübung des Widerspruchsrechts darstellen, solange eine Profilbildung weiter über das Pseudonym der IP-Adresse stattfindet. Somit dürfte die Speicherung der Suchanfragen – sofern es sich dabei um personenbezogene Daten handelt – bereits wegen des Fehlens einer Rechtsgrundlage rechtswidrig sein.

3.3.6.5.2.4 Suchanfragen als personenbezogene Daten

Fraglich ist aber, inwieweit es sich bei den Suchanfragen um personenbezogene Daten handelt. Nach § 3 Abs. 1 BDSG liegen personenbezogene Daten vor, wenn es sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person handelt.

Für die Definition des Begriffs der Bestimmbarkeit will Weichert in [Däubler et al. 2007, § 3 Rn. 3] eine weite Auslegung zugrunde legen. Sobald eine speichernde Stelle über eine Zuordnungsmöglichkeit verfügt, sollen Daten personenbezogen sein (ders. a.a.O.).

Demgegenüber ist nach Roßnagel und Scholz „Anonymität dadurch gekennzeichnet, dass für Einzelangaben zu einer Person die Wahrscheinlichkeit, dass diese der Person zugeordnet werden können, so gering ist, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet“ [Roßnagel/Scholz 2000, S. 724]. Pseudonyme hingegen erlaubten die Unterscheidung zwischen dem Befugten und dem Unbefugten durch die Erlaubnis oder Verweigerung des Zugriffs auf eine Zuordnungsregel technisch und organisatorisch abzubilden (dies. S. 725). Anonyme Daten seien keine personenbezogenen Daten, Pseudonyme nur für den Kenner der Zuordnungsregel (dies. a.a.O.). Ehemals pseudonyme oder anonyme Daten könnten auch nachträglich zu personenbezogenen Daten werden, wobei auch dann wieder die entsprechenden datenschutzrechtlichen Bestimmungen gelten sollen (dies. S. 728 f.).

3.3.6.5.2.4.1 Bei statischer IP-Adresse

Aber schon die IP-Adresse kann ein personenbezogenes Datum darstellen; nämlich jedenfalls dann, wenn es sich um eine fest zugewiesene IP-Adresse handelt[388], zumindest wenn diese bekannt ist, weil es dann auch dem Betreiber möglich ist, eine Verbindung zwischen der Suchanfrage und einer Person herzustellen. Nach Bizer in [Simitis 2006, § 3 Rn. 217], der den Personenbezug nicht von den Möglichkeiten des Diensteanbieters abhängig machen, sondern absolut definieren will, liegt auch bei den meisten dynamischen IP-Adressen ein personenbezogenes (bzw. vielmehr personenbeziehbares) Datum vor, da in der Regel die Zuordnungsmöglichkeit grundsätzlich über die Daten des Telekommunikationsanbieters (Provider) möglich sein wird.

Eine wirkungsvolle und den Anforderungen des Gesetzes Genüge tragende Pseudonymisierung ist in diesem Fall nur dann möglich, wenn die Verbindung zwischen Suchanfragen und IP-Adresse pseudonymisiert wird, also einer Art doppelter Pseudonymisierung unterliegt. Eine Speicherung der Suchanfragen inklusive der IP-Adressen und Zeitstempel ist demnach (je nach vertretener Auffassung zumindest in Einzelfällen) rechtswidrig.

3.3.6.5.2.4.2 Bei Verkettung von Anfragen

Insbesondere kann sich der Personenbezug aber auch über die Verkettung der Anfragen[389] untereinander ergeben. Damit ist die Einordnung des Datenbestandes abhängig von der Nutzung der

[387] Vgl. stellvertretend http://www.google.de/intl/de/privacy.html, Stand 14.Oktober 2005 (letzter Zugriff im Oktober 2007).
[388] https://www.datenschutzzentrum.de/material/tb/tb22/kap7.htm (letzter Zugriff im Oktober 2007).
[389] Zu IP-Adressen oder Cookies vgl. Abschnitt 3.3.6.3.

Suchmaschine. Da Suchmaschinen ein zentrales Mittel zum Auffinden von Informationen im Internet darstellen, sind insbesondere verkettete Suchanfragen naheliegenderweise geeignet, um ein umfangreiches Bild über den Nutzer zu vermitteln. In den von AOL veröffentlichten Suchanfragen finden sich Begriffe, die Rückschlüsse auf nahezu alle Lebensbereichen zulassen, angefangen von Kaufinteressen über Krankheiten bis hin zu sexuellen Vorlieben. Darüber hinaus lassen sich über die Zeitstempel der Anfragen Informationen über die Häufigkeit und Intensität der Internetnutzung gewinnen.

Hierbei ist nicht auszuschließen, dass der verkettete Datensatz Informationen enthält, die die Daten zu personenbezogenen machen. So beispielsweise dann, wenn der Nutzer nach sich selber sucht, also seinen Namen in das Formular eingibt. Zwar ist in diesem Fall nicht eindeutig, ob ein Dritter nach dem Namen gesucht hat, aber auch dann würden ein personenbezogene Daten entstehen, die die Angabe enthielten, dass nach einer bestimmten Person gesucht wurde (was wiederum verknüpft wäre mit der Information, welche Anfragen die suchende Person noch gestellt hat).

In diesem Fall ist eine Pseudonymisierung praktisch unmöglich. Der Suchmaschinenbetreiber müsste nämlich zunächst herausfinden, ob eine Suchanfrage einen (zur Identifizierung geeigneten) Namen enthalten hat, und müsste diese dann durch ein Pseudonym ersetzen. Dies dürfte sich in der Praxis deswegen als schwierig gestalten, da in diesem Fall jede Suchanfrage mit einer Liste von entsprechenden Namen abgeglichen werden müsste.

Eine Korrektur des Ergebnisses über eine zweifelhafte Fiktion einer Einwilligung bei dieser Form von aufgedrängtem Personenbezug ist jedenfalls für die Fälle ausgeschlossen, in denen ein Nutzer den Namen eines Dritten in das Suchfeld eingibt. In diesem Fall fehlt es schon an der Einwilligungsfähigkeit, da der Nutzer nicht in die Verarbeitung personenbezogener Daten Dritter einwilligen kann.

3.3.6.5.3 Ergebnis der rechtlichen Betrachtung

Auch aufgrund der Verkettungsmöglichkeiten von Suchanfragen gestaltet sich die Speicherung derselben, wie sie sich derzeitig als Praxis darstellt, als rechtswidrig. Die Anbieter könnten die Anzahl der Eingriffe durch Unterrichtung und Einräumung von Widerspruchsrechten sowie „doppelte Pseudonymisierung“ (s.o.) reduzieren. In den Fällen, in denen ein Personenbezug über den Inhalt der Suchanfrage hergestellt wird, gestaltet sich die Lage als ungleich schwieriger.

3.4 Internet-Communities

3.4.1 Einleitung

Immer mehr Menschen verbringen einen Teil ihrer Freizeit in virtuellen Communities statt mit Freunden oder Bekannten an ihrem Wohnort. Der Begriff der „virtuellen Community“ (oder Online- oder Internet-Community) wurde dabei von Howard Rheingold geprägt [Rheingold 1993]. Als eine der ersten Internet-Communities wird der 1985 von Stewart Brand und Larry Brilliant gegründete virtuelle Debattierclub „The Well“ („The Whole Earth 'Lectronic Link“) angesehen.

Rheingold beschreibt Internet-Communities als „social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace.“

Communities lassen sich durch die folgenden drei Kriterien beschreiben:

- kommunikativer Austausch von Personen, die gemeinsame Interessen und Kenntnisse verbinden;
- Integration von Inhalten in der Community und ein kommunikativer Austausch darüber;
- der Großteil der in der Community integrierten Inhalte, stammt von den Mitgliedern selbst.

Diese drei Kriterien für Communities wurden aus den insgesamt fünf Kriterien von Hagel und Armstrong abgeleitet, die eine Definition von Communities unter dem ökonomischen Aspekt geben [Hagel/Armstrong 1997].

Eine Klassifikation von Internet-Communities kann nach unterschiedlichen Gesichtspunkten erfolgen. Dieses Kapitel widmet sich den durch verschiedene Klassifikationen entstehenden Typen, stellt die unter dem Aspekt der Verkettbarkeit digitaler Identitäten interessanten Aspekte vor und beleuchtet sie aus rechtlicher Perspektive. Differenziert werden kann in diesem Zusammenhang nach der Person bzw. dem Personenkreis, der die jeweiligen Verkettungen vornimmt. Insoweit ist zunächst die Person bzw. das Unternehmen zu nennen, das die jeweilige Community betreibt. Darüber hinaus können Verkettungen personenbezogener Daten aber auch von den Mitgliedern einer Community vorgenommen werden.

3.4.2 Mitgliedschaft und Rolle

Communities leben von ihren Mitgliedern und den Aktionen, die diese mit Hilfe eines Community-Systems innerhalb der Community ausüben. Hier ist nun zu unterscheiden zwischen Communities, die eine explizite Anmeldung als Mitglied erfordern, und solchen, die auch die implizite Form des Eintritts oder Austritts aus der zugehörigen Internet-Community durch Aufnahme oder Terminierung der Teilnahme in Form von Aktionen, erlauben. Alleine über diese Teilnahme definieren sich damit die Mitglieder der Community.

Wenn die Mitgliedschaft in der Community hingegen eine Anmeldung beim Community-System erfordert, muss der Nutzer in der Regel mindestens ein Pseudonym samt Passwort zur Authentisierung wählen. Oft wird auch die Angabe einer E-Mail-Adresse zur Erreichbarkeit außerhalb der Community verlangt, an die häufig vor Freischaltung der Mitgliedschaft eine E-Mail zwecks Gültigkeitsüberprüfung und Bestätigung der Anmeldung durch das Mitglied gesendet wird. Vielfach ist die Liste der anzugebenden Daten noch wesentlich umfangreicher und weist zahlreiche personenbezogene Daten auf wie Name, Geburtsdatum usw.

Der Nutzer muss dabei meist AGBs zur Nutzung seiner Daten zustimmen. Auch Datenschutzerklärungen werden bei großen Providern von Community-Systemen meist angegeben.

Es scheint jedoch so, dass nur etwa 10 % der Mitglieder an einer Community aktiv teilnehmen [White 2001]. Die Personen, die sich im Hintergrund halten und oft nur „lesen“, werden vielfach als „Lurkers“ bezeichnet. Diese setzen sich aus Personen zusammen, die neu in der Community sind, die nie einen Beitrag veröffentlichen, oder lediglich als Besucher teilnehmen wollen.

3.4.3 Klassifikation nach Orientierung

Markus versucht, eine Klassifikation von Communities nach ihrer Orientierung vorzunehmen [Markus 2002], die im Folgenden erläutert wird.

3.4.3.1 Communities sozialer Orientierung

Communities sozialer Orientierung stellen den Ursprung aller Communities dar, aus dem sich alle anderen entwickelt haben. Sie umfassen alle Communities, die rein soziale Aspekte beinhalten. In ihnen entstehen durch die soziale Interaktion der Mitglieder miteinander umfangreiche Profile sozialer Art. Sie lassen sich weiter wie folgt unterteilen:

3.4.3.1.1 Communities zum Beziehungsaufbau

In Communities zum Beziehungsaufbau ergibt sich dieser möglicherweise aus gemeinsamen, privaten Interessen (z.B. durch ein gemeinsames Hobby, geographische Nähe oder demographische Ähnlichkeit). Damit Menschen Beziehungen zueinander aufbauen können, müssen sie miteinander vielfältig interagieren und Eigenschaften und Interessen des anderen erfahren. Dadurch entstehen für die Mitglieder gewollt umfangreiche digitale Identitäten, unter denen sie in der Community agieren. Häufig lässt sich der Effekt beobachten, dass Menschen in dieser virtuellen Umgebung wesentlich mehr private Details ausplaudern als sie dies in ihrem realen Umfeld tun. Dies geschieht unter der Annahme, in der Community in einem gewissen Sinn anonym zu sein, was jedoch immer mehr

dadurch aufgehoben wird, dass in diesen Communities neben virtuellen Beziehungen auch reale Beziehungen in Form von Freundschafts- und Paarbeziehungen aufgebaut werden. Insbesondere erfolgt in diesen Communities meist keine Trennung verschiedener Kontexte, sondern die Mitglieder offenbaren vielfältige Aspekte ihrer digitalen Identität und ihres realen Lebens.

3.4.3.1.2 Communities zur Unterhaltung

In Communities zur Unterhaltung betreiben die Mitglieder damit ein Hobby. Bei diesen Communities kann es sich um Online-Spiele, Chaträume oder ähnliche Umgebungen handeln. Zwar können auch dort neue Beziehungen aufgebaut werden, aber das Hauptmotiv für den Beitritt ist die Suche nach Unterhaltung. Dabei werden typischerweise zwar Meinungen ausgetauscht, meist aber keine derart privaten Details der digitalen Identitäten wie in Communities zum Beziehungsaufbau.

3.4.3.2 Communities professioneller Orientierung

Communities professioneller Orientierung konzentrieren sich auf ein Thema aus dem professionellen Umfeld. Sie verfolgen das Ziel, über die Grenzen der eigenen Organisation hinaus mit Personen Kontakt aufzunehmen oder mit denen Informationen auszutauschen, die für die Erfüllung ihrer eigenen Aufgaben ähnliche Informationen benötigen. Oftmals werden diese Communities auch „Knowledge Communities“ genannt. Durch die vielen, zum Teil sehr qualifizierten Mitglieder, erfolgt eine Konzentration an Wissen über spezielle Themengebiete. Diese Communities lassen sich weiter in zwei Kategorien unterteilen: Lernnetzwerke und Expertennetzwerke.

3.4.3.2.1 Lernnetzwerke

Lernnetzwerke (Forschung; Universität) haben zum Ziel, Wissen zu vermitteln. Universitäten erproben schon vielfach, sich in einem Lernnetzwerk zusammenzuschließen und ihren Studenten einen einheitlichen Lehrstoff online zu vermitteln. Dabei existiert kein direkter Kontakt miteinander, sondern Lehrstoff und die dazu gehörenden Aufgaben sind virtuell abrufbar. Wenn Probleme auftreten, kann sich der Student virtuellen Lerngruppen anschließen. um sein Anliegen zu diskutieren. Diese Systeme bieten keine wesentlich größere Verkettbarkeit als das reale Studium. Die Teilnahme an den Kursen erfordert in der Regel eine Registrierung, vor allem, wenn auch ein Leistungserwerb gewünscht ist. Da die Lerngruppen im Community-System in der Regel allen Hörern offen stehen, lassen sich Informationen über den Lernstoff effektiver verteilen, was sowohl positiv als auch negativ für den Lernerfolg gesehen werden kann.

3.4.3.2.2 Expertennetzwerke

Expertennetzwerke (Informationen/Wissen, Praxis) haben zum Ziel, das Wissen innerhalb der Community zu vergrößern und gleichzeitig eine Plattform zu schaffen, auf der Probleme und Fragen diskutiert und Lösungen ausgearbeitet werden können. Dazu sind Mitglieder notwendig, die über ein beträchtliches Wissen zu einem bestimmten Thema verfügen.

In dieser Art von Community treten bezüglich der auftretenden Daten häufig die Mitglieder als Autoren in den Hintergrund zugunsten der Inhalte, die sie produzieren und einer breiten Öffentlichkeit zur Verfügung stellen, die jeder einzelne Nutzer für sich filtern und deren Qualität selbst beurteilen muss.

3.4.3.3 Communities kommerzieller Orientierung

An dieser Stelle stehen virtuelle Communities, die sich nicht aus sozialen Motiven heraus entwickelt haben, sondern vielmehr, um Gewinn und Profit zu erzielen. Untergliedert wird der kommerziell-orientierte Typ wie folgt:

- *Business-to-Consumer (B2C)-Communities* sind (auch nach [Hagel/Armstrong 1997]) Communities, die von einem Unternehmen ins Leben gerufen wurden und angeboten werden,

um sowohl seinen Kunden als Ansprechpartner zur Verfügung zu stehen, als auch seinen Kunden die Möglichkeit zu geben, sich mit anderen Kunden über die vom Unternehmen angebotenen Produkte oder Dienstleistungen zu unterhalten. Damit haben diese Communities das Ziel, Kunden zu gewinnen, sie an das Produkt zu binden und somit die Marketingkosten gering zu halten.

- *Consumer-to-Consumer (C2C)-Communities* sind Communities, in denen sich Kunden untereinander über Produkte, Dienstleistungen und Unternehmen austauschen. Sie können von Unternehmen oder auch privat betrieben werden.
- *Business-to-Business (B2B)-Communities* dienen (auch nach [Hagel/Armstrong 1997]) dem Austausch von Unternehmen untereinander, um sie in bestimmten Bereichen zu unterstützen. Die teilnehmenden Unternehmen verfolgen dabei das Ziel, gemeinsame Strategien zu entwickeln und geeignete Geschäftspartner zu finden, um Aufträge anzunehmen bzw. zu vergeben.

Die Grenzen zwischen Consumer-to-Consumer-, Business-to-Consumer- und Business-to-Business-Communities sind fließend. Oft ist eine exakte Abgrenzung zwischen den einzelnen Communities kaum möglich.

Bei kommerziell orientierten Communities sind die auftretenden Daten meist standardisiert und die resultierenden Verkettbarkeitseigenschaften ähnlich zu denen bei E-Commerce generell. Im Wesentlichen unterscheidet sich jedoch das anwendbare Recht danach, ob es sich um eine B2C- oder eine C2C-Community handelt. Vielfach ist der Übergang zwischen diesen fließend, wofür der Begriff *Prosumer* geprägt wurde. Dieser fließende Übergang erschwert eine eindeutige rechtliche Beurteilung[390].

Einer der größten Anbieter einer C2C-Community (bei der immer mehr Consumer zum Prosumer werden) mit nach eigenen Angaben ca. 72 Millionen aktiven Mitgliedern Ende 2005 ist die Auktionsplattform eBay.[391] eBay dient dem Zweck, dass die Mitglieder untereinander Artikel verkaufen können. Registrierung und (Ver-)Kaufaktivitäten stehen unter der Kontrolle von eBay. Nach dem Verkauf eines Artikels müssen dieser sowie der dafür vereinbarte Preis ausgetauscht werden. Dieser Austausch muss fair vonstatten gehen, d.h., Käufer und Verkäufer müssen beide das erhalten, auf das sie sich geeinigt hatten.

Technische und juristische Maßnahmen, die Fairness beim Warenaustausch garantieren, sind sehr aufwändig. Da jedoch der Preis vieler Artikel relativ niedrig ist (z.B. Bücher, CDs, Computerspiele, Kleidung), entscheiden sich viele Verkäufer und Käufer zum direkten Austausch von Geld und Ware. eBay lässt ihnen zu diesem Zweck die notwendigen persönlichen Daten des anderen Mitglieds zukommen. Beim direkten Austausch über räumliche Entfernung leistet nur Nachnahmeversand die Garantie, dass entweder Bieter und Anbieter oder keiner von beiden etwas[392] erhält. Bei Geldüberweisung und normalem Postversand muss mindestens einer von beiden dem anderen einen Vertrauensvorschuss entgegenbringen. Üblicherweise überweist der Käufer dem Verkäufer den vereinbarten Gegenwert des Objektes auf sein Bankkonto, und der Verkäufer versendet nach Geldeingang das verkaufte Objekt an den Käufer. Damit wird der Vertrauensvorschuss vom Käufer entgegengebracht. Übliche außerhalb des technischen Systems sammelbare Beweise für korrektes Verhalten sind dann Überweisungs- und Versandbelege. Eine entsprechende juristische Durchsetzung der eigenen Forderungen erfordert jedoch wiederum hohen Aufwand.

---

390 Schon an dieser Stelle ist klarzustellen, dass es sich bei dem Begriff „Prosumer“ nicht um einen rechtlichen Terminus handelt: Vielmehr ist etwa aus der Sicht des Verbraucherschutzrechts die Abgrenzung zwischen Verbraucher und Unternehmer maßgeblich, hinsichtlich des Datenschutzrechts ist zu klären, ob ein Community-Mitglied die Daten ausschließlich für persönliche oder familiäre Tätigkeiten oder auch zu beruflichen oder kommerziellen Zwecken verwendet. Näheres hierzu weiter unten in rechtlichen Abschnitt dieses Kapitels unter 3.4.9.

391 http://www.ebay.com/ (letzter Zugriff im Oktober 2007).

392 Dabei ist anzumerken, dass der Empfänger der Nachnahmesendung deren Inhalt vor Bezahlung in der Regel nicht inspizieren kann, d.h., dass es möglich ist, dass sie nicht das Versprochene enthält bzw. er dies behaupten kann.

Viele dieser Warenaustausche sind erfolgreich, aber einige sind es nicht. In der eBay-Community werden fortlaufend Betrugsfälle aufgedeckt, in denen ein Mitglied vorgab, Objekte zu verkaufen, entsprechende Gegenwerte von Käufern kassierte und dann aber die angebotenen Objekte nicht auslieferte. Von den beim Internet Crime Complaint Center (IC3) in den USA 2006 gemeldeten 207.492 Beschwerden über Internetbetrug entfielen 44,9 % alleine auf Internetauktionsbetrugsfälle[393]. Obwohl die dabei verlorene Geldsumme oft niedrig ist und der aktuelle Anteil an Betrugsfällen von den insgesamt getätigten Geschäften über Auktionen gering zu sein scheint (bei eBay spricht ein Vertreter beispielsweise von weniger als 0,1 % bestätigten Fällen unter den gelisteten Angeboten [Wearden 2004]), ist die Verärgerung der einzelnen betroffenen Nutzer meist groß und trägt zur Verunsicherung aller Nutzer bei.

Hier wurden Reputationssysteme eingeführt, um Erfahrungen zwischen Käufern und Verkäufern zu sammeln, zukünftige Erfahrungen abschätzen zu können und auf dieser Basis angemessen zu reagieren. Ein solches Reputationssystem funktioniert folgendermaßen: Nach dem direkten Austausch von Geld und Ware dürfen Verkäufer und Käufer einander in der Form von Kommentaren und Noten bewerten. Diese werden zum Feedback-Profil des entsprechenden Mitglieds hinzugefügt (üblicherweise mit bewertendem Mitglied und Bewertungskontext, insbesondere Nennung der Ware). Vor dem Kauf bei einem bestimmten Verkäufer oder dem Verkauf an einen bestimmten Käufer kann jedes Mitglied sich über dessen bisheriges Bewertungsprofil informieren. Sein bisheriges Verhalten gibt einen Anhaltspunkt für sein zukünftiges. Auf Reputationssysteme wird genauer im Abschnitt 4.7.2 eingegangen.

3.4.4 Klassifikation nach Bedürfnissen

Hagel und Armstrong klassifizieren Communities über die sie vereinenden Bedürfnisse, die damit gewisse Profile der Mitglieder implizieren [Hagel/Armstrong 1997], wie im Folgenden dargestellt.

3.4.4.1 Interessengemeinschaften

In Interessengemeinschaften (engl.: „communities of interest“) befriedigen die Mitglieder ihren Austausch über ein klar abgegrenztes, allen gemeinsames Interesse. Damit ist offensichtlich, dass die pure Mitgliedschaft in einer Community ein Interessensgebiet, und damit ein bestimmtes Nutzerprofil impliziert – sowohl für Außenstehende als für die Teilnehmer der Community. Dabei kann es natürlich auch zu Angreifern kommen, die nur vorgeben, ein bestimmtes Profil zu haben, aber aus anderen Gründen der Community beitreten möchten. Zum Finden von Mitgliedern mit gemeinsamen Interessen in größeren Communities wurden von [Huberman/Franklin/Hogg 1999] technische Realisierungsmöglichkeiten einer Internet-Community vorgestellt, die es Mitgliedern ermöglichen sollen, andere Mitglieder mit gleichen Interessen zu finden. Mitglieder, die nicht die gleichen Interessen haben, erfahren die Interessen der anderen nicht. Ein zusätzliches Protokoll erlaubt es, einem Mitglied zu beweisen, dass es zu einer Gruppe mit bestimmten Interessen gehört, ohne seine eigene Identität aufzudecken. Leider gibt es jedoch auch hier keine Möglichkeit, ein Mitglied daran zu hindern, ein falsches Profil innerhalb der Internet-Community aufzubauen, das nicht seinen eigentlichen Interessen entspricht.

3.4.4.2 Phantasiegemeinschaften

In Phantasiegemeinschaften (engl.: „communities of fantasy“) befriedigen die Mitglieder ihr Bedürfnis nach Phantasie, Spiel und Unterhaltung. Mit der Schaffung neuer, virtueller Umgebungen, Identitäten, Persönlichkeiten und Geschichten können die Mitglieder neben ihrem realen Leben ein fiktives Leben in dieser virtuellen Community leben, das initial nicht verkettbar ist bzw. dessen Verkettbarkeit der Kontrolle des Nutzers obliegt. Lediglich die verwendeten technischen Systeme schränken ihn in seiner Unverkettbarkeit ein, wie noch in der Klassifikation nach verwendeter Kommunikationstechnik in Abschnitt 3.4.7 näher ausgeführt wird.

[393] Internet Crime Complaint Center: IC3 2006 Internet Crime Report, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf (letzter Zugriff im Oktober 2007)

3.4.4.3 Transaktionsgemeinschaften

In Transaktionsgemeinschaften (engl.: „communities of transaction“) befriedigen die Mitglieder ihr Shopping-Bedürfnis. Dies äußert sich im Kauf und Verkauf von Produkten oder Dienstleistungen, aber auch im aktiven Meinungsaustausch der Mitglieder über diese Produkte und Dienstleistungen. Meist werden solche Communities von Unternehmen initiiert und entstehen im Umfeld von Online-Shopping-Möglichkeiten im Internet. Auf diese Art von Communities wurde bereits in der vorigen Klassifizierung als Communities kommerzieller Orientierung in 3.4.3.3 eingegangen.

3.4.4.4 Beziehungsgemeinschaften

In Beziehungsgemeinschaften (engl.: „communities of relationship“) befriedigen die Mitglieder ihr Bedürfnis danach, besondere oder insbesondere gemeinsame Lebenserfahrungen mit anderen zu teilen. Dadurch entstehen meist enge, persönliche Beziehungen der Mitglieder, die sich in einer gemeinsam geteilten virtuellen Kultur äußern können. Auf diese Art von Communities wurde bereits in der vorigen Klassifizierung als Communities sozialer Orientierung zum Beziehungsaufbau in 3.4.3.1.1 eingegangen.

3.4.5 Klassifikation nach Teilnehmerprofilen

Hagel und Armstrong unterscheiden Internet-Communities auch nach den typischen Teilnehmerprofilen [Hagel/Armstrong 1997]. Im privaten Bereich gibt es insbesondere die folgenden Kategorien:

- *Geographische Communities* werden durch den physischen Ort definiert, an dem die Teilnehmer (seien es Endnutzer oder Unternehmen) sich befinden oder für den sie Interesse zeigen. Dies kann eine Webseite zur Stadt, zu einem Stadtteil oder einer Region sein, die Community-Dienste enthält bzw. anbietet.
- *Demographische Communities* bestehen aus Teilnehmern, die gemeinsame demographische Merkmale (z.B. Altersgruppe, Geschlecht, Familienstand, Kinderanzahl) aufweisen und von daher ein gemeinsames Interesse am Austausch mit anderen in ähnlicher Situation haben. Sehr beliebt sind beispielsweise Foren für Jugendliche oder Eltern.
- *Interessengeleitete Communities* definieren sich aus dem gemeinsamen Interesse der Teilnehmer an einem Thema (ein Hobby, der Beruf, eine Krankheit etc.) aufgrund ihres Teilnehmerprofils.

Interessant bezüglich der auftretenden Daten ist, dass bei einer Einteilung der Communities nach Teilnehmerprofilen bereits der Besuch einer bestimmten Community, und erst recht die Mitgliedschaft darin, in der Regel eine Verkettbarkeit des entsprechenden Teilnehmerprofils zum Nutzer impliziert.

3.4.6 Klassifikation nach dem Betreiber

Auch nach ihren Betreibern können Communities unterschieden werden. Während Unternehmen Communities hauptsächlich anbieten, um daraus wirtschaftliche Vorteile und/oder Erlöse zu erzielen, steht bei einem Betrieb durch Privatpersonen eher das Interesse an einem Thema oder der Wunsch nach einem Gemeinschaftsgefühl im Vordergrund. Auch Vereine und andere Organisationsstrukturen können das Internet nutzen, um ihre gemeinsamen Aktivitäten effizienter zu organisieren und Außenstehende darüber zu informieren.

Bei vielen der heute anzutreffenden Communities ist ein Schutz vor dem Betreiber kaum möglich. Zwar lässt sich mittlerweile die Anonymität oder Pseudonymität des Nutzers mit einfachen Mitteln sichern (z.B. durch Verwendung eines Anonymisierungsdienstes). In Punkten wie Vertraulichkeit und Integrität ist der Nutzer aber oft dem Betreiber und möglichen Angreifern ausgeliefert. Vielfach ist selbst die Nutzung von Communities per SSL nicht möglich.

3.4.7 Klassifikation nach verwendeter Kommunikationstechnik

Das verwendete Community-System zur Kommunikation der Community-Mitglieder sowie die eigentliche Internet-Community, die mit Hilfe dieses Community-System miteinander interagiert, sind voneinander zu unterscheiden. Häufig nutzt dieselbe Community verschiedene Kommunikationstechniken. Dennoch eignen sie sich auch zur Klassifikation von Communities, da sie die Verkettbarkeit von Nutzern entscheidend beeinflussen:

3.4.7.1 Newsgroup/Usenet

In *Newsgroups* oder im *Usenet* werden die Informationen, die von den Nutzern bereitgestellt wurden, an einer zentralen Stelle gesammelt und können von dort von einem beispielsweise in E-Mail-Clients integrierten Newsreader ohne Registrierung abgerufen und vom Nutzer gelesen werden. Um die vielen existierenden Newsgroups zu unterscheiden, wurden neun internationale Hauptkategorien mit verschiedenen Themenbereichen geschaffen. Daneben gibt es auch nationale Kategorien, die Newsgroups für ein bestimmtes Land zusammenfassen. In ihnen gibt es dann weitere Unterkategorien, die innerhalb eines Themenbereiches die Gruppe weiter unterteilen. Zwecks Kontaktierbarkeit außerhalb der Newsgroup bietet es sich an, eine gültige E-Mail-Adresse zum Verfassen von Texten zu verwenden. Dies wird in der Regel jedoch nicht überprüft. Durch die Einteilung in die Kategorien ergeben sich meist Interessengemeinschaften oder Expertennetzwerke.

3.4.7.2 E-Mail

Ein *Newsletter* ist die einfachste Art, mit den Besuchern einer virtuellen Community Kontakt aufzunehmen. Für das Abonnement eines Newsletters ist eine Registrierung beim Anbieter mit Hinterlassen der E-Mail-Adresse und ggf. weiteren Informationen nötig. Der Inhalt eines Newsletters wird durch den Anbieter bestimmt und bietet keine Interaktionsmöglichkeiten. Da es sich bei einem Newsletter in den meisten Fällen um frei zugängliche Informationen handelt, sind die entsprechenden Interessen zu den Empfängern verkettbar.

Mailinglisten bieten die Möglichkeit multidirektionaler Kommunikation zwischen den Abonnenten. Neben der Möglichkeit, innerhalb einer eigenen Domain eine Mailingliste einzurichten, gibt es auch große Anbieter, die die technische Plattform für private Mailinglisten bereitstellen. Die anfallenden Daten werden durch die Nutzer selbst generiert und können zu ihrer E-Mail-Adresse verkettet werden. Eine besondere Möglichkeit der Verkettung kommt dabei dann dem Anbieter zu, der die technische Plattform für private Mailinglisten bereitstellt.

3.4.7.3 Webforen

Webforen bilden die Newsgroups im Internet (Web 1.0) ab.[394] Der Besucher eines solchen Forums kann auf die vorhandenen zentral auf einem Webserver gespeicherten Informationen zugreifen oder selbst Informationen beisteuern.

Es ist oft möglich, Themen in geschützten Bereichen zu erstellen, auf die nur ein kleiner Kreis von Mitgliedern zugreifen kann, bzw. Nachrichten können nur an einzelne Nutzer gesendet werden. Der Provider erlaubt Kommunikation einzelner Nutzer miteinander zunächst nur mittels Nachrichten über das Webforum statt durch direkte E-Mails. Dies schützt die Anonymität der Nutzer voreinander und schützt kritische Inhalte vor den Blicken Unberechtigter. Dadurch liegen dem Dienstanbieter selbst jedoch alle Daten, die über das Webforum ausgetauscht werden, vor: Öffentlich lesbare sowie auch private Nachrichten. Die Nutzer können meist zusätzlich keine Verschlüsselungs- und Anonymisierungstechnologien anwenden, wie sie dies bei herkömmlicher E-Mail-Kommunikation könnten.

[394] Viele Betreiber nutzen die technische Infrastruktur phpBB (http://www.phpBB.com/; letzter Zugriff im Oktober 2007) zur Realisierung ihres Webforums.

3.4.7.4 Chat/Messenger

Chat ist eine synchron geführte Kommunikation mit einem oder mehreren Teilnehmern. Die technische Realisierung ist dabei nur auf kleine Gruppen ausgerichtet:

- Für *Internet Relay Chat (IRC)* oder *Instant Messaging (IM)* sind ein Chat-Server und eine Client-Software notwendig, die auf den Rechnern der Nutzer installiert sein muss. Gechattet wird hier auf verschiedenen Kanälen. Die Netze unterscheiden sich in regionalen Schwerpunkten, Sprachen, Themen und angebotenen Services. Das Chat-System ist textbasiert, erlaubt jedoch über weitere Kommandos auch den Austausch von Dateien und sonstigen Informationen über eine *Direct Client-to-Client-Verbindung (DCC)* zweier User. Programme dieser Art sind der Instant Messenger von ICQ, der AOL Instant Messenger, der Microsoft Messenger oder der Yahoo! Messenger. Früher war Nachrichtenversand zwischen den Systemen nicht möglich; erst neuere Programme, die alle vier Messenger-Systeme vereinen, stellen diese Funktion zur Verfügung. Ebenso wurde die Kommunikation vom geschriebenen Text auf so genannte Voice-Chats (Voice-over-IP) erweitert.
- Beim *Web-Chat* loggen sich die Benutzer direkt auf dem Chat-Server ein. Dies geschieht durch Chat-Software, die beispielsweise bereits durch Browser-Plugins direkt in die HTML-Seiten integriert ist. Der Nutzer benötigt in diesem Fall kein eigenes Client-Programm im Gegensatz zu typischen IRC- oder IM-Anwendungen.

Bei allen IM-Systemen ist eine Registrierung auf dem jeweiligen Betreiberserver notwendig, der die Aufgabe hat, die Nutzerdaten zu speichern und zwischen den einzelnen Mitgliedern zu vermitteln. Bei den Nutzerdaten handelt es sich im minimalen Fall um ein Pseudonym und eine Identifikationsnummer. Zudem besteht immer die Gefahr, dass der Betreiber Daten wie z.B. die IP-Adresse zusätzlich mit erfasst. Alle heute existierenden IM-Systeme nutzen das IRC-Protokoll[395], das nicht abhörsicher ist. Es existiert eine IRC-SSL-Protokollerweiterung, mit der eine verschlüsselte Kommunikation zwischen Server und Nutzer möglich ist. Dies sichert die Geheimhaltung und Integrität der Kommunikation zwischen zwei Benutzern vor externen Angreifern, nicht jedoch vor dem Betreiber.

Abhilfe gegen dieses Problem schafft das SILC-Protokoll[396]: Mit ihm ist eine Ende-zu-Ende-Verschlüsselung zwischen zwei Nutzern möglich, wobei es die Identifikation nicht mehr nach Identifikationsnummern, sondern nach öffentlichen Schlüsseln vornimmt. Die ersten praxistauglichen Versionen wurden bereits für Linux veröffentlicht.

3.4.7.5 Peer-to-Peer-Technik, insbesondere Filesharing

Unter Peer-to-Peer (P2P) versteht man Netzstrukturen, bei denen im Gegensatz zu Client-Server-Konzepten alle angeschlossenen Rechner gleichbedeutend sind. Jeder in einem P2P-Netz angeschlossene Rechner kann also seine Hard- oder Software anderen Rechnern zur Verfügung stellen oder die der anderen Rechner nutzen.

Filesharing-Systeme erlauben Nutzern über ein Netz den Austausch von vielfältigen Daten (z.B. Musik, Filmen, Computerprogrammen usw.). Napster war das erste populäre Filesharing-System zum Austausch von Musik bis 2000 einige Musikbands Klage gegen Napster einreichten und die Tauschbörse daraufhin aufgelöst wurde[397]. Versuche, Napster in eine kostenpflichtige Tauschbörse zu konvertieren, schlugen lange Zeit fehl, da nur wenige Musikfirmen bereit waren, ihre Musik zu lizenzieren. Mittlerweile hat sich Napster[398] jedoch zu einem kostenpflichtigen Musikdownload-Anbieter gewandelt, der seinen Kunden zu einem Pauschaltarif den legalen Download von Musikfiles anbietet, damit aber keine Community mehr darstellt.

Da die Datenmengen, die Nutzer austauschen möchten, meist sehr hoch sind, basieren die meisten Filesharing-Systeme inzwischen auf P2P-Technik (z.B. Gnutella, Kazaa). Dabei kann jeder Teilnehmer Dateien auf seinem Rechner anderen zur Verfügung stellen. Die Verteilung einer Datei erfolgt häufig

[395] http://www.faqs.org/rfcs/rfc1459.html (letzter Zugriff im Oktober 2007).
[396] http://silcnet.org/support/documentation/specs/ (letzter Zugriff im Oktober 2007).
[397] http://www.heise.de/newsticker/meldung/19224/ (letzter Zugriff im Oktober 2007).
[398] http://www.napster.de/ (letzter Zugriff im Oktober 2007).

über verschiedene Peers als Zwischenstufen oder Teile einer Datei parallel von verschiedenen Peers. Dadurch verkompliziert sich die rechtliche Verantwortung im Falle von illegalen Datentransfers, z.B. aufgrund von Urheberrechtsverletzungen.

Insbesondere Open-Source-Software wird schon seit längerem unter anderem über Filesharing verteilt. Aber auch viele nicht an einen Vertrag gebundene Musiker und Künstler nutzen Filesharing, um ihre Werke zu veröffentlichen und mit relativ geringem Aufwand sehr viele Menschen zu erreichen.

Ein Nutzer kann in der Regel über die IP-Adresse, mit der er am P2P-Netz teilnimmt, identifiziert werden. Unter gerichtlich verfügter Mitwirkung der Internetprovider können Personen, die urheberrechtlich geschützte Dateien austauschen, über ihre IP-Adresse identifiziert werden.

Außer Frage steht jedoch, dass trotz des berechtigten Interesses der Musikindustrie weiterhin grundsätzlich der anonyme Austausch von selbstverfassten Daten möglich sein soll. Das Ziel anonymer P2P-Konzepte (z.B. Gnunet[399]) ist es deshalb, dass die im System befindlichen Inhalte nicht mehr einzelnen Nutzern zugeordnet werden können.

3.4.7.6 Online-Spiele

Auch die Mitwirkenden in Online-Spielen bilden Communities. Abhängig von ihrer Struktur lassen sich drei hauptsächliche Typen von Online-Spiele unterscheiden: die privaten Netze, geschlossene Systeme sowie Massive-Multiplayer-Online-Games (MMOGs). Die folgenden Abschnitte erläutern ihre Charakteristika.

3.4.7.6.1 Private Netze

Bei privaten Netzen wird die Verbindung zum Spielen einzig zwischen den Spielern selber aufgebaut. Entweder sind sämtliche eingebundenen Rechner gleichberechtigt eingebunden oder einer der Teilnehmer wird zum Host-System bestimmt, über den die Spielvorgänge laufen. Wurden früher hierzu eigene Netze aufgebaut, wird heute in der Regel für die Verbindung der Rechner das Internet verwendet. Die Spielprogramme sollten so gestaltet werden, dass z.B. ein Abhören der Kommunikation zwischen den Spielern durch Dritte unterbunden wird. Auch sollten die Datenübermittlungsvorgänge für alle Spieler transparent sein.

3.4.7.6.2 Geschlossene Systeme

Geschlossene Spielsysteme werden von externen Dritten betrieben z.B. Xbox Live, Playstation Home, zentrale Game-Server) und können für unterschiedliche vom Anbieter definierte Spiele genutzt werden können; Erweiterungen für den Nutzer sind nur im vom Anbieter angebotenen Rahmen möglich.

Online-Spielsysteme wie Xbox Live können zahlreiche Daten über das Spielverhalten ihrer Nutzer sammeln. Der Nutzer kann diese selber einsehen, aber auch anderen zur Einsicht freischalten, sofern diese Daten nicht schon standardmäßig freigegeben sind. Damit haben dann alle Spieler Einblick in Daten wie zuletzt gespielte Spiele, erreichte Spielziele oder besondere Leistungen im Spiel. Bereits der Umstand, dass jemand ein bestimmtes Spiel spielt, kann sensibel sein, z.B. im Rahmen der Killerspiel-Debatte könnten Spieler von Egoshootern als potenzielle Amokläufer gesehen werden oder Nachteile bei Bewerbungen erleiden. Insbesondere aber die Analyse des Verhaltens von Personen in einem Spiel kann zahlreiche Aussagen über den Spieler hervorbringen. Hierbei ist zu erwarten, dass Informationen, die über virtuelle Identitäten gesammelt werden, mit Daten aus der Offline-Welt verkettet werden, um so Aussagen über die realen Personen treffen zu können. Dies betrifft nicht nur das Reaktionsvermögen, sondern auch die Mentalität, mit der Spielaufgaben angegangen und gelöst werden.

Die Kommunikation der Spieler untereinander mittels Textbotschaften, Sprache oder Bildern stellt bei geschlossenen Systemen meist ein zentrales Element dar. Hierbei sind u.a. Grundsätze des Fern-

[399] http://gnunet.org/ (letzter Zugriff im Oktober 2007).

meldegeheimnisses zu beachten. Andererseits haben die Anbieter ein Interesse daran, dass diese Systeme nicht dazu genutzt werden, um andere Spieler zu beleidigen oder anders zu belästigen.

Einige Systeme lassen sich auch mit Webcams verbinden, so dass man z.B. Mitspieler mit Videobild sehen kann. Bei Xbox Live ist es in der Vergangenheit sehr oft vorgekommen, dass Spieler dieses dazu nutzen, um obszöne Gesten oder nackte Geschlechtsteile den Mitspielern zu präsentieren. In Anbetracht des Jugendschutzes könnte daher eine strengere Überwachung und Rückverfolgung (z.B. Protokollierung) notwendig werden. Diese müsste datenschutzgerecht gestaltet werden (z.B. Möglichkeit des unbeobachtbaren Privatgesprächs).

In Online-Spiele sind teilweise bereits Reputationssysteme integriert, bei denen Mitspieler bewertet werden können bzw. Beschwerden eingereicht werden können. Diese Systeme sollten mehrseitig sicher ausgestaltet werden, so dass der Nutzer bei einer schlechten Bewertung eines Mitspielers nicht fürchten muss, selber schlecht bewertet zu werden. Dabei sollte allerdings auch Missbrauch so weit wie möglich unterbunden werden.

Zu untersuchen ist, ob (z.B. in Anbetracht des § 13 Abs. 6 Telemediengesetz) eine anonyme Nutzung von Online-Spielen möglich sein muss und wie diese in der Praxis umgesetzt werden kann, insbesondere angesichts der verbreiteten Speicherung von IP-Adressen und des Kontextes von zunehmenden – oft invasiven – Maßnahmen zum Schutz vor Raubkopierern.

3.4.7.6.3 Massive-Multiplayer-Online-Games (MMOGs)

Bei den Massive-Multiplayer-Online-Games MMOGs (z.B. World of Warcraft oder Second Life) werden den Spielern virtuelle Welten zur Verfügung gestellt. Im Rahmen von Massive-Multiplayer-Online-Games, insbesondere wenn sie Freiheiten wie bei Second Life bieten, können umfangreiche Interessenprofile erstellt werden, je nachdem, welche virtuellen Gegenden dort besucht und welche Aktionen vorgenommen werden. Dass zahlreiche bekannte Firmen Second Life dazu nutzen, um Marketing für ihre Produkte zu betreiben (z.B. Adidas, Mercedes Benz, Springer Verlag), zeigt, dass Online-Spielen ein Werbewert zugesprochen wird. Für die Betreiber dieser virtuellen Geschäfte ist es entsprechend interessant, das Verhalten der Besucher zu analysieren und diese Informationen für weitere Marketingaktivitäten zu nutzen.

Dabei ist es auch möglich, programmgesteuerte Avatare zu generieren, deren Aufgabe es ist, alle Informationen zu protokollieren, die sie in der virtuellen Welt erreichen können. Dies können nicht nur Verhaltensmuster von anderen Avataren sein, sondern auch deren Gespräche. Insbesondere durch längerfristige Beobachtungen kann es möglich sein, dass die Identitäten von virtuellen Personen aufgedeckt werden.

Die Nutzer von MMOGs haben meist ein gesteigertes Interesse daran, dass ihre virtuelle Identität nicht mit der in der realen Welt in Verbindung gebracht wird. Daher ist hier besonders darauf zu achten, dass keine Aufdeckung dieser Pseudonyme erfolgt. Wünschenswert wären grundsätzlich Systeme, die vollständig anonym genutzt werden können. Allerdings ergäben sich dann Probleme mit der Abrechnung und insbesondere mit Vandalismus im System. Sofern Straftaten im virtuellen Raum (z.B. Beleidigungen, sexuelle Belästigung, Betrug) nicht technisch verhindert werden können, müsste ein System derart gestaltet sein, dass es in solchen Fällen eine Aufdeckung der Täter ermöglicht, um Geschädigten zu ihrem Recht zu verhelfen.

Systeme wie Second Life erlauben auch Geschäfte zwischen den „Spielern“. Selbst Firmen und öffentliche Einrichtungen sind dort bereits vertreten. Damit hat ggf. nicht nur der Betreiber der virtuellen Welt die Datenschutzgesetze zu beachten, sondern auch der (geschäftlich auftretende) Mitspieler. Bei der Betrachtung ist zunächst zu unterscheiden hinsichtlich der realen steuernden Person und der virtuellen Identität. So könnte die virtuelle Identität, wenn sie erst einmal eine gewisse Reputation aufgebaut hat, ein eigenes „Interesse“ an informationeller Selbstbestimmung haben. Juristisch ist dies noch genauso ungeklärt wie die Frage, inwieweit diese auf die reale Person hinter der virtuellen Identität durchschlägt.

Aus rechtlicher Sicht besteht ein grundlegendes Problem in der Bestimmung des überhaupt einschlägigen Rechts für Phantasiegemeinschaften. Die meisten der existierenden Systeme werden im Aus-

land, meist auch außerhalb der EU, betrieben. Die Frage ist dann, inwieweit überhaupt deutsches oder europäisches Recht Anwendung findet. Diese Problematik wird noch verschärft, wenn die Spiele P2P-Technik verwenden und die Spieler selbst Dienste anbieten. Insoweit sei auf die Ausführungen von [Krasemann 2006] verwiesen.

3.4.7.7 Wiki-Software

Eine Wiki-Software ermöglicht Community-Mitgliedern, Webseiten der Community einfach mit einem Browser zu editieren und so gemeinsame Inhalte der Community zu schaffen. Oft schließt sich eine Versionsverwaltung an, die Änderungen aufzeichnet und verschiedene Bausteine und Versionen der Webseite in einer Datenbank sammelt. Damit kommt diese Software häufig für Expertennetzwerke zum Einsatz. Ein bekanntes Wiki ist die Wikipedia[400], in der Informationen zu allen möglichen Begriffen zusammengetragen werden.

3.4.8 Verkettbarkeit in und über Communities

3.4.8.1 Verkettbarkeit zur physischen Person

Verbunden mit der Steigerung der Internetnutzung möchten Nutzer die sozialen Netzwerke, in denen sie real leben, auch online nutzen oder gar neu bilden. Viele Communities unterstützen dies durch Freundeslisten innerhalb der Community, Verknüpfung verschiedenster Datentypen (wie Fotos). Viele Einträge werden mit Schlagworten versehen und kommentiert, so dass die Inhalte und Nutzer immer stärker miteinander verkettet werden und sich Gleichgesinnte schneller finden können. Communities zum Beziehungsaufbau widmen sich vielfach nicht nur einem dafür beschränkten Interessensgebiet, sondern dienen der Selbstdarstellung der Mitglieder, um Kontakte zu initiieren[401] oder zu re-initiieren, wenn Menschen sich im realen Leben aus den Augen verloren haben[402]. Beide Formen des Kontaktwunsches gründen auf der zunehmenden Mobilität der Nutzer im physischen Leben: Bei realen Veränderungen im Leben der Nutzer bietet wenigstens die Community Konstanz bzw. stellt diese wieder her. Umgekehrt können auch Communities physische Mobilität verursachen, indem Nutzer andere Mitglieder treffen und damit eine Verkettbarkeit der digitalen Identität innerhalb der Community zu ihrer physischen Person herstellen.

Während es einem Nutzer bei anderen Diensten des Internets (z.B. E-Mail, Shopping) häufig frei steht, für welchen Dienst er sich entscheidet, gilt dies für Communities meist nicht. Bedingt durch den realen Freundeskreis bleibt vielen Nutzern häufig keine Wahl als sich auch bei der Community zu registrieren, wo ihr reales Umfeld aktiv ist[403], um nicht von Informationen ausgeschlossen zu werden. Auch wenn ein Nutzer bei der Registrierung noch die Wahl haben sollte, so gilt dies häufig nicht mehr nach einer gewissen Mitgliedszeit, da seine Daten (Freundeslisten, Einträge, Nachrichten, etc.) fest mit dem gewählten Community-Betreiber zusammenhängen und er den Kontakt zu den entsprechenden Mitgliedern nicht verlieren möchte.

Die in Communities zur Verfügung gestellten Informationen bilden den Alltag ihrer Nutzer häufig sehr nahe an der Realität ab. Viele Dienstanbieter beziehen dazu Orts- und Zeitinformationen in ihr Angebot mit ein. Beispiel ist die Möglichkeit, Fotos zu mit dem genauen Aufnahmeort zu verknüpfen. Auch einige Kamerahersteller nutzen schon GPS-Sensoren, um die Ortsdaten in Fotos vollautomatisch einzubetten.

Die damit verkettbaren Informationen erlauben es, Reisen der die Fotos bereitstellenden Mitglieder genau zu verfolgen. Durch zeitnahe Veröffentlichung mit mobilen Geräten lässt sich hierbei jederzeit erfahren, wo sich der Nutzer gerade aufhält.

[400] http://www.wikipedia.org/ (letzter Zugriff im Oktober 2007).
[401] Z.B. bei http://www.xing.com/ (letzter Zugriff im Oktober 2007).
[402] Z.B. bei http://www.stayfriends.de/ (letzter Zugriff im Oktober 2007).
[403] Z.B. Studenten bei http://www.studivz.de/ (letzter Zugriff im Oktober 2007).

Schließlich ist es auch möglich, unter Verwendung Community-interner Daten gezielte Anfragen an Suchmaschinen zu stellen und so weitere Informationen über die jeweilige Person zu erlangen – diese können dann wiederum mit den bereits vorhandenen Daten verkettet werden.

3.4.8.2 Verkettbarkeit über mehrere Communities

Die Verbindungen eines Nutzers beschränken sich ebenso wie im realen Leben jedoch nicht nur auf eine Community, sondern die meisten Nutzer sind in zahlreichen Communities, sowohl gleicher als auch unterschiedlicher Ausrichtung, oft aber mit sich ergänzenden Diensten aktiv. Querverweise auf andere Quellen des Web sind im Zuge von Web 2.0 nicht mehr nur Hyperlinks auf diese, sondern auch Verknüpfungen zwischen den verschiedenen Pseudonymen, die ggf. zur selben Person gehören.

Viele Nutzer werden dabei auch selbst aktiv und nutzen die steigenden Möglichkeiten, die das Internet ihnen bietet, anderen Informationen zur Verfügung zu stellen. Vor einigen Jahren war noch eigener Webspace nötig, um eine eigene Homepage zu erstellen, auf der man dann auch verschiedene Medientypen (wie Musik, Bilder, Texte etc.) anbieten konnte. Auf Webseiten anderer Betreiber keine Beiträge oder meist nur textueller Art wie z.B. in Gästebüchern erstellen. Heute gibt es hingegen zahlreiche Dienste, die Webspace bereitstellen und Nutzer technisch unterstützen, anderen Informationen der verschiedensten Medientypen bereitstellen zu können sowie Links zu anderen Nutzer und deren Seiten zu setzen. Dabei hat der Nutzer als Adressaten meist Mitglieder seines sozialen Netzwerks, aber auch andere, die er gerne dazu zählen würde, im Sinn.

Für die oben beschriebene Entwicklung hat sich der Begriff des Web 2.0 etabliert. Die anscheinend der Softwareentwicklung entliehene Zählweise beschreibt jedoch weniger einen festen Entwicklungsschritt des Internets, sondern ist eher einen fortlaufenden Prozess, dessen Entwicklung politisch und rechtlich aktiv zu begleiten ist.

Die Nutzer, die im Web 2.0 Informationen suchen, stehen oft hilflos vor Unmengen von Datenmengen, aus denen sie die für sich relevanten herausfiltern müssen. Durch die vielfältigen Möglichkeiten der Interaktion mit anderen im Internet, lassen sich Informationen eben auch nicht mehr passiv auf Webseiten nur lesen, sondern können in Communities auch erfragt werden. Dazu ist aber zunächst die geeignete Community zu finden.

Die Nutzer, die im Web 2.0 zur Verfügung stellen möchten, müssen ebenfalls erst den geeigneten Ort dazu suchen, wo sie möglichst viele andere erreichen, die sie zu den Adressaten zählen möchten.

Aus beiden Gründen zeigen Nutzer und Betreiber von Communities zahlreiche Bestrebungen, die Trefferrate für „ihre“ Daten bei Suchmaschinen zu erhöhen und damit gewollte Verkettung zu erreichen. Um Wiedererkennbarkeit in verschiedenen Communities zu gewährleisten, nutzen viele Nutzer in all ihren unterschiedlichen Communities dasselbe Pseudonym.

3.4.8.3 Verkettbarkeit innerhalb einer Community

Die Betreiber großer Community-Plattformen des Web 2.0 versuchen, einen möglichst großen Markt abzudecken, um die Effekte des sozialen Netzwerks zu erhöhen. Es gibt derzeit mindestens 41 Dienste mit mehr als einer Million Mitglieder[404]; der größte Anbieter MySpace[405] hat nach eigenen Angaben mehr als 174 Millionen Mitglieder.

Zur Steigerung der Mitgliedszahl und zur Bindung der Nutzer an die Community versuchen die großen Betreiber Alleinstellungsmerkmale herauszuarbeiten, die den Nutzer an die Plattform binden und ihn animieren sollen, möglichst viele Dienste dort zu nutzen. Die Anbieter von Internet-Communities bieten dabei vielfach auch Dienste an, die bereits anderweitig unabhängig von der Community vorhanden und durch die Nutzer einfach verwendbar wären: Populäres Beispiel ist, dass E-Mails durch Nachrichten auf den jeweiligen Plattformen ersetzt werden, so dass Nachrichten zwischen Mitgliedern nicht mehr direkt fließen, sondern über den Community-Betreiber, der diese häufig dann doch per E-

[404] Siehe http://en.wikipedia.org/wiki/List_of_social_networking_websites (letzter Zugriff im Oktober 2007).
[405] http://www.myspace.com/ (letzter Zugriff im Oktober 2007).

Mail an den jeweiligen Nutzer zustellt. Während dies den Vorteil der Pseudonymität der Nutzer gegenüber einander hat, erlangt der Community-Betreiber Kontrolle über private Kommunikation. Anders als bei E-Mail-Diensten können Nutzer meist keine Verschlüsselungs- und Anonymisierungstechniken einsetzen oder deren Einsatz wird stark erschwert.

Community-Betreiber nehmen neben dieser Breite ihres Angebotes allerdings auch eine Anpassung an verschiedene Zielgruppen vor, um die Nutzerzahl zu steigern: International tätige Communities versuchen insbesondere eine Sprachanpassung je nach adressiertem Land[406].

Diese Bindung an eine Community mit vielen Diensten vergrößert das Profil eines Nutzers innerhalb einer Community erheblich. Gleichzeitig werden durch Anpassung an die Zielgruppen wie Sprache Mitglieder bereits profilmäßig unterschieden. Auch wenn viele Betreiber die Nutzer darauf hinweisen, dass sie innerhalb der Community personenbezogene Daten vermeiden sollten[407], bestehen sie selbst auf Angabe korrekter Daten bei der Registrierung und erhalten damit große Mengen an verkettbaren personenbezogenen Daten.[408]

Die Integration der Dienste in eine Plattform und die Pseudonymität der Nutzer erschwert Mitgliedern den Austritt aus einer Internet-Community, wenn sie nicht den Kontakt zu den anderen Mitgliedern verlieren wollen.

3.4.8.4 Geschäftsumfeld

Das Web 2.0 wird zunehmend als lukratives Geschäftsumfeld gesehen. Der Anbieter bietet lediglich die Infrastruktur, den Inhalt selbst erstellen die Nutzer mit ihren Beiträgen. So lassen sich mit relativ geringem Aufwand hohe Nutzerzahlen erreichen.

Diese Nutzerzahlen sind für Werbepartner interessant: So zahlte Google 2006 an die News Corporation ca. 900 Millionen Dollar[409], um für 3 Jahre und 9 Monate exklusive Suchmaschine auf den von der News Corporation betriebenen Internetseiten, zu denen auch die Community MySpace gehört, zu sein.

Immer mehr werden Communities auch von großen Unternehmen aufgekauft: News Corporation kaufte MySpace für ca. 580 Millionen Dollar, Google kaufte YouTube[410] für ca. 1,65 Milliarden Dollar, Holzbrinck kaufte StudiVZ[411] für ca. 100 Millionen Euro.

Es wird bereits vielfach in den Medien diskutiert, wie Communities einen solchen Marktwert erreichen können und Gewinne damit erwirtschaftet werden. Dazu gibt es prinzipiell nur die Möglichkeit durch die Mitglieder selbst oder durch Externe. Ersteres bedeutet Zahlung von Mitglieds- oder Transaktionsgebühren[412], die aber bei Communities sozialer Orientierung kaum bezahlt werden, da die Nutzer bereits durch Beiträge zur Community beitragen. Oder das Mitglied wird explizit oder implizit zum Objekt von Marketing, sei es durch klassische (inzwischen jedoch oft personalisierte) Werbeanzeigen auf den Seiten des Dienstes oder durch die Weitergabe von Daten über die Mitglieder an andere Dienste.

3.4.8.5 Risiken

Zahlreiche Risiken ergeben sich insbesondere aus der Verkettbarkeit digitaler Identitäten zu realen Personen. Dies betrifft zum einen den beruflichen Bereich:

406 Z.B. http://www.netlog.com/ (letzter Zugriff im Oktober 2007)
407 Z.B. Netlog: http://de.netlog.com/go/inside/view=privacyStatement (letzter Zugriff im Oktober 2007).
408 Z.B. Netlog: http://de.netlog.com/go/inside/view=generalConditions (letzter Zugriff im Oktober 2007).
409 http://www.spiegel.de/wirtschaft/0,1518,430602,00.html (letzter Zugriff im Oktober 2007).
410 http://www.youtube.com/ (letzter Zugriff im Oktober 2007).
411 http://www.studivz.de/ (letzter Zugriff im Oktober 2007).
412 eBay (http://www.ebay.de/) verlangt beispielsweise für die Eröffnung und den Abschluss von Auktionen eine Gebühr.

- Firmen haben aufgrund von Einträgen in Weblogs, die sich negativ über die Firma äußerten, Mitarbeiter entlassen[413]. Offenbar ist vielen Nutzern nicht bewusst, dass die Meinungsäußerung digital eben nicht der im physischen Bereich gleichkommt, wo nur ein kleiner Freundeskreis adressiert wird.
- Arbeitgeber oder von ihnen beauftragte Headhunting-Agenturen benutzen in zunehmendem Maße Suchmaschinen wie Google, um Informationen über Bewerber zu erlangen.[414] Zahlreiche Nutzer versuchen zwar, die Suchergebnisse zu ihrer Person vor einer Bewerbung zu beschönigen, aber zum einen ist vorstellbar, dass Agenturen schon vorab versuchen, Profile junger Arbeitnehmer mit hoher Wahrscheinlichkeit der Bewerbung zu erlangen, und zum anderen sind einmal veröffentlichte Daten schwer rückrufbar. Durch eine gewollte hohe Verkettbarkeit gewünschter Attribute lassen sich ungewünschte Attribute jedoch zumindest ansatzweise zurückdrängen.

Im privaten Bereich sind die folgenden unerwünschten Auswirkungen auf Betroffene zu beobachten:

- Im privaten Bereich stellt Stalking ein Problem dar, was einerseits virtuell, andererseits durchaus auch physisch passieren kann. Häufige Opfer sind hierbei sind Frauen[415] und Kinder[416].
- Aufgrund der mangelnden Authentisierungsmöglichkeiten im Internet und der Freiheit der Pseudonymwahl kann die Verwendung von Pseudonymen durch mehrere Personen (als vorsätzlicher Pseudonymdiebstahl, absichtliche Weitergabe von Pseudonymen oder versehentliche Kollision) unerwünschte Konsequenzen für einen oder mehrere Beteiligte haben. Nutzer fassen ihr Pseudonym desweilen als anscheinend eindeutig auf, unter dem sie bekannt sind, ggf. auch über mehrere Communities hinweg, und nutzen es, um implizite Reputation aufbauen. Dabei haben sie jedoch in der Regel keinerlei Rechte an diesem Pseudonym und sind nicht davor gefeit, dass andere Nutzer sich in anderen Communities unter diesem Pseudonym bekannt machen und damit ihre eigene Reputation aufbauen. Dies wird problematisch, wenn Communities sich immer mehr überlappen und zwei Personen um dasselbe Pseudonym streiten. Insoweit sei hier nochmals darauf hingewiesen, dass auch ein Pseudonym namensrechtlichen Schutz genießen kann. Dies setzt allerdings voraus, dass es bereits Verkehrsgeltung erlangt hat.[417] Ist dies der Fall, so kann der Inhaber des Pseudonyms von einem anderen, der dieses ebenfalls in den betreffenden Verkehrskreisen verwendet, verlangen, dass er dies künftig unterlässt[418].

3.4.9 Abschließende rechtliche Betrachtung von Communities

3.4.9.1 Allgemeines

Bei Internet-Communities handelt es sich regelmäßig um Telemedien im Sinne des Telemediengesetzes. Zu diesen zählen nämlich alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste oder Rundfunk sind[419]. Nachfolgend wird kurz dargestellt, unter welchen Voraussetzungen der Anbieter eines solchen Telemediendienstes personenbezogene Daten miteinander verketten darf und wie die Verkettung von Daten durch die Mitglieder einer Community rechtlich zu bewerten ist.

[413] Beispielsweise Friendster: Blog-Betreiber feuert Mitarbeiter wegen Blog-Eintrag (http://www.zdnet.de/news/tkomm/0,39023151,39125557,00.htm (letzter Zugriff im Oktober 2007).
[414] http://web.bsu.edu/careers/spotlight/articles/05-06/issue2/facebook.htm (letzter Zugriff im Oktober 2007).
[415] Beispielsweise: „Neuer Ärger um StudiVZ: Sex-Stalker im Studentennetz“, abrufbar unter http://www.spiegel.de/netzwelt/web/0,1518,450866,00.html (letzter Zugriff im Oktober 2007).
[416] Beispielsweise: Families sue News Corp. and MySpace after children abused by adult MySpace users, 18.01.2007 (http://www.wtnh.com/Global/story.asp?S=5956321 (letzter Zugriff im Oktober 2007)).
[417] Maxem-Entscheidung, siehe bereits oben im juristischen Grundlagenteil unter 2.3.3.3.3.2.
[418] §§ 12, 1004 BGB.
[419] § 1 Abs. 1 S. 1 TMG.

3.4.9.2 Verkettung(en) durch den Betreiber einer Community

3.4.9.2.1 Rechtsgrundlagen für eine Verkettung personenbezogener Daten

Wie bereits erwähnt, handelt es sich bei Internet-Communities zumeist um Telemedien im Sinne des Telemediengesetzes. Wie stets im Internetkontext stellt sich auch hier zunächst die Frage nach dem jeweils anwendbaren Recht. Sofern deutsches Recht einschlägig ist, gelten für die Anbieter solcher Dienste regelmäßig[420] die bereichsspezifischen Datenschutzregelungen der §§ 11 ff. des Telemediengesetzes (TMG) und ergänzend hierzu die Vorschriften des Bundesdatenschutzgesetzes. Nach § 12 Abs. 1 TMG darf ein Diensteanbieter personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit das Telemediengesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat. Hinsichtlich der gesetzlichen Erlaubnistatbestände differenziert das Telemediengesetz sodann in §§ 5 und 6 zwischen Bestands- und Nutzungsdaten.

3.4.9.2.1.1 Anwendbares nationales Recht

Da es im Bereich des Internets vielfach zu einer grenzüberschreitenden Verarbeitung personenbezogener Daten kommt, stellt sich hier oft die Frage nach dem im konkreten Einzelfall anwendbaren nationalen Recht. Hinsichtlich des Anbietens von Telemedien sieht das Telemediengesetz selbst in seinem § 3 Regelungen bezüglich des jeweils anwendbaren Rechts vor. Diese Regelung ist in Umsetzung der sog. E-Commerce-Richtlinie 2000/31/EG[421] der Europäischen Union erlassen worden und bestimmt, dass innerhalb der Bundesrepublik Deutschland niedergelassene Diensteanbieter und ihre Telemedien den Anforderungen des deutschen Rechts auch dann unterliegen, wenn die Telemedien in einem anderen Staat innerhalb des Geltungsbereichs der E-Commerce-Richtlinie geschäftsmäßig angeboten oder erbracht werden (sog. Herkunftslandprinzip).

Allerdings bestimmt § 3 Abs. 3 Nr. 4 TMG, dass die genannte Vorschrift gerade nicht für das Datenschutzrecht gilt. Insoweit sind also die allgemeinen Regelungen des Bundesdatenschutzgesetzes anwendbar. Einschlägig ist hier § 1 Abs. 5 BDSG, wonach für die Anwendbarkeit des deutschen Datenschutzrechts von wesentlicher Bedeutung ist, ob der Sitz der verantwortlichen Stelle innerhalb oder außerhalb des Europäischen Wirtschaftsraumes (EWR)[422] liegt.

Befindet sich der Sitz der Daten verarbeitenden Stelle nicht in Deutschland, aber innerhalb des EWR, so ist das deutsche Datenschutzrecht grundsätzlich nicht einschlägig. Es kommt dann vielmehr das Recht des Staates, in dem die verantwortliche Stelle ihren Sitz hat, zur Anwendung (sog. Sitzprinzip)[423]. Etwas anderes gilt allerdings dann, wenn die verantwortliche Stelle ihren Sitz zwar außerhalb von Deutschland hat, aber eine Niederlassung[424] in der Bundesrepublik Deutschland betreibt. In diesem Falle gilt dann ausnahmsweise deutsches Datenschutzrecht.

Hat die verantwortliche Stelle ihren Sitz hingegen außerhalb des EWR, so ist für die Anwendbarkeit des deutschen Datenschutzrechts der Ort, an dem die Datenverarbeitung vorgenommen wird,

---

[420] Nach § 11 Abs. 1 TMG gelten diese bereichsspezifischen Regelungen aber nicht für die Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien, soweit die Bereitstellung solcher Dienste im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder innerhalb von oder zwischen nichtöffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

[421] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr")

[422] Zum Europäischen Wirtschaftsraum zählen neben den EU-Staaten auch noch Norwegen, Island und Liechtenstein.

[423] § 1 Abs. 5 S. 1 BDSG.

[424] Nach Erwägungsgrund 19 der EU-Datenschutzrichtlinie 1995/46/EG ist Voraussetzung für eine Niederlassung in diesem Sinne die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung. Näheres zum Begriff der Niederlassung findet sich bei Dammann in [Simitis 2006, § 1 Rn. 203 ff.].

maßgeblich (sog. Territorialitätsprinzip)[425]. Es ist also beispielsweise dann deutsches Recht anwendbar, wenn sich der Sitz der Daten verarbeitenden Stelle in den Vereinigten Staaten befindet, die Daten aber in einem in Deutschland befindlichen EDV-System verarbeitet werden[426]. An dieser Stelle sei im Übrigen noch kurz angemerkt, dass eine Übermittlung personenbezogener Daten aus Deutschland heraus an Stellen außerhalb des Europäischen Wirtschaftsraum nach § 4b f. BDSG nur dann zulässig ist, wenn neben der für jede Datenverarbeitung obligatorischen Rechtsgrundlage noch weitere Voraussetzungen vorliegen[427].

3.4.9.2.1.2 Verkettung(en) aufgrund einer Einwilligung des Nutzers

Rechtsgrundlage für eine Verkettung personenbezogener Daten kann zunächst eine Einwilligung des jeweiligen Community-Mitglieds sein. § 13 Abs. 2 TMG sieht vor, dass eine solche Einwilligung unter bestimmten Umständen auch elektronisch erteilt werden kann. Hierzu muss der Diensteanbieter sicherstellen, dass

- der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

Zu beachten ist in diesem Zusammenhang auch das sog. Koppelungsverbot des § 12 Abs. 3 TMG: Hiernach darf der Diensteanbieter die Bereitstellung von Telemedien nicht von der Einwilligung des Nutzers in eine Verwendung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telemedien nicht oder in nicht zumutbarer Weise möglich ist.

3.4.9.2.1.3 Gesetzlicher Erlaubnistatbestand für eine Verkettung von Bestandsdaten

Bei Bestandsdaten handelt es sich um Daten, die im Zusammenhang mit einem Vertragsverhältnis über die Nutzung von Telemedien anfallen. Nach § 14 Abs. 1 TMG darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Anbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind.

3.4.9.2.1.4 Gesetzlicher Erlaubnistatbestand für eine Verkettung von Nutzungsdaten

Nutzungsdaten fallen hingegen im Zusammenhang mit der Inanspruchnahme von Telemedien an. Bei ihnen handelt es sich insbesondere um Merkmale zur Identifikation des Nutzers, um Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung sowie um Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Nach § 15 Abs. 1 TMG darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Darüber hinaus darf er nach Abs. 2 dieser Vorschrift Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemedien zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.

Schließlich darf der Diensteanbieter nach § 15 Abs. 3 TMG für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien pseudonyme Nutzungsprofile erstellen, sofern der Nutzer dem nicht widerspricht. Diese Nutzungsprofile dürfen nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden. Dies hat der Dienste-

[425] § 1 Abs. 5 S. 2 BDSG.

[426] Einzelheiten zur Beantwortung der Frage, wann Daten im Inland erhoben, verarbeitet oder genutzt werden und damit deutsches Datenschutzrecht anwendbar ist, finden sich bei Dammann in [Simitis 2006, § 1 Rn. 220 ff.].

[427] Ausführlich hierzu etwa Dammann in [Simitis 2006, §§ 4b und c].

anbieter durch technische und organisatorische Vorkehrungen sicherzustellen. Führt der Anbieter trotz des gesetzlichen Verbots ein Nutzungsprofil mit Daten über den Träger des Pseudonyms zusammen, so handelt es sich hierbei um eine Ordnungswidrigkeit, die mit einer Geldbuße bis zu 50.000 EUR geahndet werden kann[428].

3.4.9.2.2 Transparenz hinsichtlich einer Verkettung von Nutzungsdaten

§ 13 TMG statuiert neben anderen Pflichten des Diensteanbieters auch solche zur Sicherstellung der Transparenz der Datenverarbeitung:

Nach Abs. 1 der Vorschrift muss der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs in allgemein verständlicher Form über die Art der personenbezogenen Daten sowie über Umfang und Zwecke der Erhebung und Verwendung dieser Daten unterrichten[429]. Außerdem ist der Nutzer auch über eine eventuelle Verarbeitung seiner personenbezogenen Daten in Staaten außerhalb des Anwendungsbereichs der EU-Datenschutzrichtlinie 1995/46/EG zu informieren. Des Weiteren ist der Nutzer auch bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, zu Beginn dieses Verfahrens zu unterrichten. Schließlich muss der Inhalt der jeweiligen Unterrichtung für den Nutzer jederzeit abrufbar sein.

Nach § 13 Abs. 5 TMG muss der Diensteanbieter dem Nutzer zudem eine Weitervermittlung zu anderen Diensteanbietern anzeigen.

Schließlich muss der Diensteanbieter nach Abs. 7 der Vorschrift dem Nutzer nach Maßgabe des bereits vorgestellten § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten erteilen. Dabei kann der Nutzer verlangen, dass diese Auskunft auf elektronischem Wege erteilt wird.

3.4.9.3 Verkettung(en) durch die Mitglieder einer Community

Verkettungen können nicht nur durch den Telemedienanbieter (also den Betreiber der jeweiligen Internet-Community), sondern auch durch die einzelnen Mitglieder einer Community vorgenommen werden. Werden insoweit personenbezogene Daten zu kommerziellen Zwecken verarbeitet, so sind – sofern deutsches Recht anwendbar ist[430] – die Vorschriften des Bundesdatenschutzgesetzes für nicht-öffentliche Stellen zu beachten[431]. Erhebt, verarbeitet oder nutzt das Community-Mitglied die Daten hingegen ausschließlich für persönliche oder familiäre Tätigkeiten, so fällt dies gem. § 1 Abs. 2 Nr. 3 BDSG nicht unter das Anwendungsbereich des BDSG. Wie bereits erwähnt, gilt dies auch hinsichtlich sog. Prosumer[432], also einer Personengruppe, die zwischen den einfachen Verbrauchern und beruflichen Anwendern steht. Da für diesen Personenkreis im Bereich des Rechts keine speziellen Regelungen bestehen, sind hier stets die auch für alle anderen Personen maßgeblichen Vorschriften anzuwenden. So ist im Falle einer Verarbeitung personenbezogener Daten durch Prosumer stets zu prüfen, ob personenbezogene Daten ausschließlich für persönliche bzw. familiäre oder nicht vielmehr doch zu kommerziellen Zwecken verarbeitet werden.

Im Zusammenhang mit der Verarbeitung personenbezogener Daten zu „rein privaten“ Zwecken sei außerdem noch darauf hingewiesen, dass die zunehmende Digitalisierung, Miniaturisierung und Vernetzung von IT sowie die sich permanent steigernde Speicher- und Verarbeitungsleistung gängiger Rechner auch Privatpersonen dazu in die Lage versetzt, umfassende Datenbestände zu speichern, auszuwerten oder anderweitig zu verwenden. Wie soeben gesehen, fallen solche „rein privaten“

[428] § 16 Abs. 2 Nr. 6, 3 TMG.

[429] In der Praxis geschieht dies überwiegend über Datenschutzhinweise auf der jeweiligen Webseite, auch wenn fraglich ist, ob bei einem solchen Prozedere der gesetzlichen Unterrichtungspflicht in vollem Umfang genügt wird.

[430] Vgl. hierzu bereits oben unter 3.4.9.2.1.1.

[431] Diese sind bereits oben unter 3.3.1.1vorgestellt worden. Die datenschutzrechtlichen Bestimmungen des Telemediengesetzes gelten hingegen nur im Verhältnis von Telemedienanbieter und -nutzer.

[432] Bei diesem Terminus handelt es sich um ein aus den englischen Begriffen „professional“ und „consumer“ gebildetes Kunstwort.

Verarbeitungen personenbezogener Daten gegenwärtig nicht unter die datenschutzrechtlichen Vorschriften. Insoweit ließe sich darüber nachzudenken, ob aus den zunehmenden Möglichkeiten der Datenverarbeitung auch für einzelne Privatpersonen zukünftig Handlungsbedarf für den Gesetzgeber resultiert.[433]

3.4.9.4 Fazit

Im Bereich der Internet-Communities treten neben den jeweiligen Betreibern vielfach auch die Mitglieder als Verketter digitaler Daten und Identitäten in Erscheinung. Hier muss in Fällen mit Auslandsbezug zunächst geklärt werden, welches nationale Recht überhaupt anwendbar ist. Gilt deutsches Recht, so sind dabei hinsichtlich Verkettungen durch die Community-Betreiber in der Regel die bereichsspezifischen Vorschriften des Telemediengesetzes einschlägig. Für Mitglieder, die personenbezogene Daten zu kommerziellen Zwecken verketten, gelten hingegen die Vorschriften des BDSG. Schließlich unterfallen Verkettungen personenbezogener Daten, die Community-Mitglieder lediglich zu persönlichen oder familiären Zwecken vornehmen, de lege lata nicht dem Anwendungsbereich der Datenschutzgesetze.

[433] So vertritt etwa [Roßnagel 2007, S. 192 ff.] die Meinung, dass angesichts einer in den nächsten Jahren sukzessive Realität werdenden allgegenwärtigen Datenverarbeitung (Ubiquitous Computing) eine vollständige Ausnahme privater Datenverarbeitung von der Geltung des Datenschutzrechts künftig nicht mehr zu rechtfertigen sein wird. Eine private Datenverarbeitung solle aber de lege ferenda nicht vollständig dem Datenschutzrecht unterworfen werden, vielmehr müsse untersucht werden, welche Einzelregelungen des Datenschutzrechts Anwendung finden sollen.

4 Analyse von Techniken und Methoden bezüglich Verkettung

4.1 Einleitung

Bezüglich Verkettung von Daten können technische Konzepte in zwei Zielrichtungen eingesetzt werden:

1. zum Ermöglichen einer Kontrolle über die Verkettbarkeit von Daten aus nicht offensichtlich zusammengehörigen Quellen, oder
2. zum Feststellen von Gemeinsamkeiten (Verkettungen) in vorhandenen Datenbeständen.

Beide Zielrichtungen sind voneinander abhängig. Mit Techniken für die erste Zielrichtung wird versucht, die für Verkettungsvorgänge zur Verfügung stehenden Daten so zu strukturieren bzw. gezielt einzuschränken, dass nur ein gewünschter Teil der Verkettungsmöglichkeiten verbleibt. Techniken für die zweite Zielrichtung sollen diese verbleibenden Verkettungsmöglichkeiten ausnutzen.

Es werden Techniken für beide Zielrichtungen vorgestellt, wobei der Schwerpunkt gemäß dem Fokus dieser Arbeit auf Techniken der ersten Zielrichtung (Kontrolle der Verkettbarkeit) liegt.

Im Abschnitt 4.2 zu Data Warehousing und Data Mining wird ein Überblick über Methoden zum Finden von Verkettungen in bestehenden Datenbeständen gegeben. Weiterhin werden in den Abschnitten 4.3 und 4.4 mit Biometrie und RFID zwei Methoden beispielhaft erläutert, mit deren Hilfe personenbezogene Daten akquiriert werden können. Im Abschnitt 4.5 werden daraufhin grundlegende technische Konzepte vorgestellt, die zum einen die Vertraulichkeit der Kommunikationsumstände (also im Wesentlichen der personenbezogenen Daten des Nutzers) in Kommunikationsnetzen, insbesondere im Internet, sichern helfen. Zum anderen werden Konzepte vorgestellt, die eine verifizierbare Zurechenbarkeit von Aktionen zu Nutzern in solchen Netzen sicherstellen. Darauf aufbauend werden Konzepte erläutert, die Zurechenbarkeit trotz Vertraulichkeit der personenbezogenen Daten des Nutzers ermöglichen.

Der Abschnitt 4.6 beschäftigt sich dann mit den Möglichkeiten eines nutzergesteuerten Identitätsmanagements, das es dem Nutzer bis zu einem gewissen Grad ermöglicht, Verkettungen unter Bedingungen zu stellen. In Abschnitt 4.7 folgen Ausführungen zu Reputationssystemen in Internet-Marktplätzen, wo durch eine Verkettung von Bewertungen durch Dritte eine Reputation aufgebaut werden kann.

Je nach Aussagekraft der zur Verfügung stehenden personenbezogenen Daten kann Verkettbarkeit bzw. Unverkettbarkeit jeweils mit einer bestimmten Sicherheit erreicht werden. In Abschnitt 4.8 werden Methoden zum Messen von Verkettbarkeit für verschiedene Anwendungen und aus Sicht verschiedener Akteure im System beschrieben.

In Abschnitt 4.9 werden Beispiele für Anwendungen bzw. Konzepte für Anwendungen beschrieben, die eine Kontrolle der Verkettbarkeit im jeweiligen Kontext ermöglichen. Schließlich werden in Abschnitt 4.10 technische Möglichkeiten zur Entkettung von Daten vorgestellt.

4.2 Data Warehousing und Data Mining

4.2.1 Einleitung

Die immer weiter fortschreitende Digitalisierung und globale Vernetzung haben während der letzten Jahre bisher unvorstellbare Möglichkeiten einer Verkettung von Daten geschaffen. Immer kostengünstigere Speicherbausteine ermöglichen die Aufbewahrung immer umfangreicherer Datenbestände, die aus technischer Sicht nahezu unbegrenzt miteinander verkettet werden können. Die bloße Speicherung – auch exorbitant großer Datenmengen – stellt heute also kein Problem mehr dar, die Herausforderung besteht jetzt vielmehr in einer effizienten Nutzbarmachung und Analyse dieser Datenbestände. Sowohl staatliche als auch private Stellen haben ein immer größer werdendes

Interesse daran, die bei ihnen verfügbaren Daten auf für sie relevante Informationen hin zu auszuwerten. Bei Data Warehousing und Data Mining handelt es sich um Techniken und Methoden, die genau dies ermöglichen. Deshalb sind sie gerade für Unternehmen – etwa im Bereich des Customer Relationship Management (CRM) – von großer ökonomischer Bedeutung.

4.2.2 Data Warehousing

In Unternehmen fallen bei nahezu allen betrieblichen Abläufen operative Daten an, die zunächst einmal nur in den entsprechenden operativen Datenbeständen gespeichert werden. Diese sind an spezifische Software und dieser zugrundeliegenden Datenstrukturen gebunden, weshalb die in ihnen gespeicherten Daten einer bereichsübergreifenden Auswertung grundsätzlich nicht zugänglich sind. Um eine solche übergreifende Auswertung operativer Daten dennoch zu ermöglichen, bedienen sich immer mehr Unternehmen der Strategie des sog. Data Warehousing.

Der Begriff *„Data Warehousing“* bezeichnet ein Konzept, das darauf abzielt, eine zentrale Datenbank mit allen in einer Organisation vorhandenen Daten aufzubauen und diese dort dauerhaft vorzuhalten, um sie jederzeit auswerten und analysieren zu können.[434] In einem zentralen „Daten-Lagerhaus“, dem Data Warehouse, werden die operativen Daten aller oder zumindest mehrerer Unternehmensbereiche integriert und aggregiert. Dieser zentrale Datenpool ersetzt die operativen Datenbestände jedoch nicht, sondern bildet einen zusätzlichen, von diesen strikt getrennten Datenbestand.[435]

In ein Data Warehouse finden vielfach nicht nur die operativen Daten des jeweiligen Unternehmens Eingang, vielmehr werden diese meist noch um zusätzliche, von externen Anbietern erworbene Daten ergänzt. Nicht zuletzt deshalb nimmt ein solches Daten-Lagerhaus vielfach bereits nach kurzer Zeit gewaltige Dimensionen an, wodurch der Datenbestand zunehmend unübersichtlicher wird und eine Auswertung einen immer größer werdenden Zeitaufwand erfordert. Aus diesem Grunde werden Data Warehouses zumeist in kleinere, anwendungsspezifisch erstellte und redundant gehaltene Einheiten aufgespalten, für die sich die Bezeichnung *Data Mart* etabliert hat.[436]

Die Integration und Aggregation von Daten in Data Warehouses stellt im Übrigen eine optimale Voraussetzung für ein effektives Data Mining dar.

4.2.3 Data Mining

Ein Data Warehouse bzw. Data Mart kann zunächst einmal mittels einfacher Reports und herkömmlicher Analysetools ausgewertet werden. Diese Tools lassen sich unter dem Begriff *„On-line Analytical Processing (OLAP)“* zusammenfassen und ermöglichen die konkrete Beantwortung zuvor aufgeworfener Fragestellungen.[437] Mit anderen Worten geht es hier also um die Bestätigung oder das Verwerfen bestimmter Hypothesen. Diese Werkzeuge sind jedoch nicht dazu in der Lage, im Rahmen einer Auswertung komplexer Datenbestände bislang verborgene Zusammenhänge offenzulegen und neue Hypothesen zu generieren. Dies wird vielmehr erst durch die Methode des sog. Data Mining ermöglicht.

Unter dem Begriff *„Data Mining“* („Datenbergbau“) versteht man Verfahren zur Analyse komplexer Datenbestände mit Hilfe bestimmter Algorithmen, deren Ziel in der Aufdeckung verborgener Muster oder Trends und damit in der Generierung neuer Wissenszusammenhänge besteht.[438]

Der Begriff des Data Mining bezeichnet kein bestimmtes Verfahren, sondern eine Vielzahl unterschiedlicher Analyse- und Steuerungsinstrumente. Die gegenwärtig am weitesten verbreiteten Data-Mining-Verfahren[439] sind:

---

[434] Zum Begriff und zu weiteren Einzelheiten siehe [Frosch-Wilke 2003] sowie Scholz in [Roßnagel 2003, S. 1841 Rn. 17 ff.].

[435] Scholz in [Roßnagel 2003, S. 1841 Rn. 18].

[436] [Frosch-Wilke 2003, S. 599].

[437] Scholz in [Roßnagel 2003, S. 1842 Rn. 24]. Umfassende Erläuterungen hierzu finden sich bei [Frosch-Wilke 2003, S. 601 f.].

[438] Zum Begriff und zu weiteren Einzelheiten siehe Scholz in [Roßnagel 2003, S. 1843].

- die visuelle Datenexploration,
- die Cluster-Analyse,
- Methoden des induktiven Lernens und
- künstliche neuronale Netze (KNN).

Bei der sog. visuellen explorativen Datenanalyse werden Daten graphisch abgebildet, wodurch Beziehungen zwischen den abgebildeten Daten visuell erschlossen werden können. Ziel der Cluster-Analyse ist die Ermittlung unterschiedlicher Gruppen von Objekten, die einander in bestimmter Hinsicht ähnlich bzw. unähnlich sind. Durch die Methoden des induktiven Lernens sollen Klassen von Daten beschrieben oder Regeln zur Klassifizierung neuer Datenklassen erstellt werden (Letzteres wird z.B. durch die Erstellung von Entscheidungsbäumen realisiert). Künstliche neuronale Netze schließlich sollen die im menschlichen Gehirn stattfindenden Entscheidungsabläufe simulieren.

Im Übrigen können die skizzierten unterschiedlichen Verfahren sowie weitere Techniken auch miteinander kombiniert werden. Ob eine solche Kombination auch sinnvoll ist, richtet sich nach der jeweils in Rede stehenden Aufgabenstellung.

Festzuhalten bleibt, dass ein Data Mining – anders als herkömmliche Analysemethoden – die Beantwortung von Fragen ermöglicht, die zuvor (noch) gar nicht gestellt worden sind. Konkret geht es Unternehmen, die Data-Mining-Verfahren nutzen, beispielsweise um ein frühzeitiges Erkennen von Trends, eine Effektivierung ihres Marketings durch die Zuordnung von Kunden zu bestimmten Kundenklassen oder um die Prognose eines bestimmten Verhaltens von Kunden (z.B. zur Ermöglichung einer exakteren Abschätzung bestimmter Risiken).[440]

4.2.4 Fazit

Ein kombinierter Einsatz von Data Warehousing und Data Mining ermöglicht es, zuvor separierte Datenbestände in zentralen Datenpools zu aggregieren und aus den hierdurch generierten umfangreichen Daten-Lagerhäusern neue relevante Informationen herauszufiltern. Es geht also um die Ermöglichung umfangreicher Verkettungen digitaler Daten und um deren effiziente Auswertung. Diese Verkettungs- und Analysemöglichkeiten stellen aus Sicht von Unternehmen der Privatwirtschaft ein nützliches Werkzeug dar. Data Warehousing und Data Mining führen aber auch zu neuen Risiken und Gefahren für das Grundrecht auf informationelle Selbstbestimmung. Spezifische Gefährdungslagen bestehen insbesondere hinsichtlich des Zweckbindungs- und des Transparenzgrundsatzes, der (Nicht-)Einhaltung gesetzlicher Löschungspflichten und des Verbots automatisierter Einzelentscheidungen.[441] Datenschutzrechtlich problematisch sind Data Warehousing und Data Mining allerdings nur dann, wenn die dergestalt verarbeiteten Daten einen Personenbezug aufweisen. Wenn ein Unternehmen die beiden Techniken für unverzichtbar hält, bleibt ihm insofern nämlich immer noch die Möglichkeit, anonymisierte oder pseudonymisierte Daten für deren Realisierung zu verwenden.[442]

[439] Ausführliche Erläuterungen zu den vier nachfolgend genannten Verfahren finden sich bei [Frosch-Wilke 2003, S. 603 f.].

[440] Scholz in [Roßnagel 2003, S. 1844 Rn. 32].

[441] Einzelheiten zu möglichen Datenschutzgefährdungen zu Data Warehousing und Data Mining finden sich bei Scholz in [Roßnagel 2003, S. 1845 ff.].

[442] Deshalb hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Hersteller und Anwender entsprechender Verfahren bereits im Jahr 2000 dazu aufgerufen, „solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.“ Die entsprechende Entschließung findet sich z.B. unter http://www.datenschutz-berlin.de/doc/de/konf/59/datawa.htm (letzter Zugriff im Oktober 2007).

4.3 Biometrie

4.3.1 Grundlagen

Biometrie[443] wird zur Authentisierung von Personen angewandt. Hierzu werden Merkmale aus zentral oder dezentral gespeicherten Referenzdaten mit Merkmalen aus aktuellen Sensordaten verglichen. Das Vergleichen (auch *Matching* genannt) kann entweder 1:1 gegen einen spezifischen Referenzdatensatz (Verifikation) oder 1:*n* gegen den Inhalt einer Referenzdatenbank (Identifikation) erfolgen. Anschließend wird das Ergebnis des Vergleichs im Sinne einer Ja-Nein-Entscheidung bewertet (*Match* oder *Non-Match*). Abbildung 7 stellt dies schematisch dar.

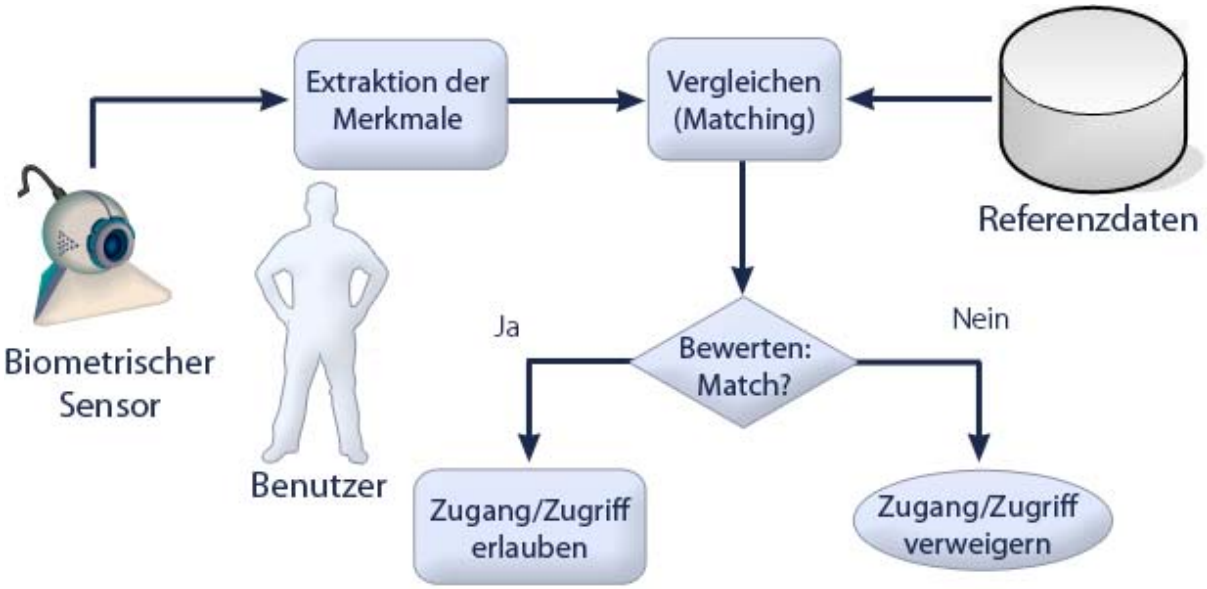


Abbildung 7: Schematische Darstellung einer biometrischen Zugangs-/Zugriffskontrolle

Referenzdaten können auf unterschiedliche Weise gespeichert werden: als so genanntes Template, bei dem nur die für das Vergleichen benötigten Merkmale gespeichert werden, oder als so genannte Rohdaten, bei denen es sich in vielen Fällen um digitale Bilder handelt. Templates sind häufig herstellerspezifisch (proprietär). Sie können i.d.R. nur mit einem speziellen mathematischen Algorithmus aus biometrischen Rohdaten erzeugt werden. Auch für das Vergleichen von Sensordaten und Referenzdaten werden angepasste Algorithmen verwendet. Die Verwendung von biometrischen Rohdaten als Referenz lässt mehr Flexibilität zu – so kann mit unterschiedlichen Algorithmen zur Extraktion von Merkmalen und verschiedenen Vergleichsalgorithmen gearbeitet werden.

4.3.2 Biometrische Daten und Verkettung

Verkettung ist sowohl über Sensor- als auch über Referenzdaten möglich. Biometrische Rohdaten können unmittelbar identifizierend sein – so kann etwa anhand eines Gesichtsbildes eine Person auch ohne Einsatz von Technik erkannt werden.

Werden in zwei Datenquellen die gleichen biometrischen Referenzdaten (Templates oder Rohdaten) gespeichert, so ist eine Verkettung ohne Einsatz biometrischer Systeme einfach durch Vergleichen der digitalen Daten beider Datenquellen möglich. Liegen in einer Datenquelle Templates eines bekannten Formates und in der anderen biometrische Rohdaten vor, so ist unter Einsatz eines bio-

[443] Die Grundlagen der Biometrie sind in zahlreichen Publikationen beschrieben, u.a. [Nolde/Leger 2002] oder http://www.bromba.com/faq/biofaqd.htm (letzter Zugriff im Oktober 2007).

metrischen Systems eine Verkettung möglich (1:*n*-Vergleich, Identifizierung). Die Folgen einer solchen Verkettung können noch weitreichender für den Betroffenen sein, wenn biometrische Daten zusammen mit anderen personenbezogenen Daten gespeichert werden.

Einige biometrische Systeme können ohne Mitwirkung oder sogar Kenntnisnahme des Betroffenen eingesetzt werden. Dies ist insbesondere bei der Kopplung von Kamera- oder Videoüberwachungssystemen mit biometrischen Systemen unter Nutzung geeigneter Referenzdaten möglich.[444] Solche Systeme bieten die Möglichkeit der Überwachung (Tracking) der Betroffenen unter Aufzeichnung von Bewegungs- und Aufenthaltsprofilen.

Templates bekannter Formate können genutzt werden, um biometrische Merkmale nachzubilden. Dies wurde für Fingerabdruck-Templates gezeigt, aus denen sich Vorlagen für Fälschungen von Fingerabdrücken errechnen lassen, die vom biometrischen System nicht mehr vom Original unterschieden werden können – vorausgesetzt, das System erkennt nicht, dass das Merkmal von keinem lebenden Finger stammt. In diesem Fall stimmen originaler Fingerabdruck und Fälschung nicht überein – ein forensischer Experte würde die Unterschiede sofort erkennen.[445]

Ein spezieller, Biometrie-bezogener Verkettungsaspekt ist, dass biometrische Rohdaten und möglicherweise verfahrensbedingt auch einige Templateformate Informationen beinhalten, die für Verifikation bzw. Identifikation nicht benötigt werden. Diese werden auch als *überschießende Informationen* bezeichnet. In vielen Fällen habe diese Informationen Gesundheitsbezug und sind daher nach geltendem Datenschutzrecht (BDSG) als „besondere Arten personenbezogener Daten“ durch spezielle Regelungen geschützt. Als Beispiele seien für die Rohdaten bei der Gesichtsgeometrie (Fotos des Gesichtes, die z.B. hinsichtlich Kopfhaltung, Verdeckung und Beleuchtung unter normierten Bedingungen aufgenommen wurden) genannt:

- das Marfan-Syndrom[446];
- Erkrankungen des Nervensystems wie Schlaganfall[447] oder Gesichtslähmung[448];
- das Down-Syndrom [449];
- Gelbsucht[450].

Infolge der verwendeten Methode (Auswertung von Geometrieeigenschaften des Gesichts, einschl. Symmetrie) muss vermutet werden, dass Informationen mindestens statistischer Art zu geometrieverändernden Krankheiten auch in allen Templateformaten enthalten sind. Dies betrifft die ersten drei genannten Beispiele. Es wurde bereits demonstriert, dass überschießende Informationen automatisiert aus Rohdaten extrahiert werden können [Graevenitz 2006].

4.4 Radio Frequency Identification (RFID)

4.4.1 RFID-Technik

Der englische Begriff *„Radio Frequency Identification“* bezeichnet eine Technik zur Identifikation von Objekten durch kontaktloses Auslesen von an diesen Objekten angebrachten *Transpondern*, so

[444] Siehe BSI-Studie BioP I unter http://www.bsi.de/literat/studien/biop/ (letzter Zugriff im Oktober 2007) und http://www.heise.de/newsticker/meldung/84260/ (letzter Zugriff im Oktober 2007).

[445] Siehe http://www.bromba.com/knowhow/temppriv.htm (letzter Zugriff im Oktober 2007) und http://chris.fornax.net/biometrics.html (letzter Zugriff im Oktober 2007).

[446] Siehe z.B. http://www.uniklinik-freiburg.de/hkz/live/KlinischeSchwerpunkte/ks-gef/marf.html (letzter Zugriff im Oktober 2007).

[447] Siehe http://www.schlaganfall-hilfe.de/index.php?option=com_content&task=view&id=59&Itemid=68 (letzter Zugriff im Oktober 2007).

[448] Siehe z.B. http://www.gesundheitpro.de/Gesichtslaehmung-Krankheiten-A050829ANONI012962.html (letzter Zugriff im Oktober 2007).

[449] Siehe z.B. http://www.lebensgeschichten.org/dsyndrom/trisomie03.php (letzter Zugriff im Oktober 2007).

[450] Siehe z.B. http://www.asklepios.com/globaleindikationen/GlobaleIndikationenInnereMedizin/lebererkrankungen.htm (letzter Zugriff im Oktober 2007).

genannten *„Tags“*, per Funk. Die Transponder bestehen dabei aus einem Chip zur Speicherung und ggf. Verarbeitung von Daten und Kommandos sowie einer Antenne zum Senden und Empfangen. RFID-Systeme bestehen in der Regel aus den Transpondern, Sende- und Empfangsanlagen (meist Lesegeräte oder Reader genannt, können aber entsprechende RFID-Chips auch beschreiben) und einem Hintergrundsystem zur Datenverarbeitung. Die vom Lesegerät empfangenen Daten der Transponder werden an ein Hintergrundsystem weitergegeben, das diese auswertet und ggf. weitere Kommunikationen mit dem Transponder, Operationen auf Datenbanken oder andere Aktionen auslöst. Abbildung 8 zeigt die Bestandteile eines RFID-Systems.

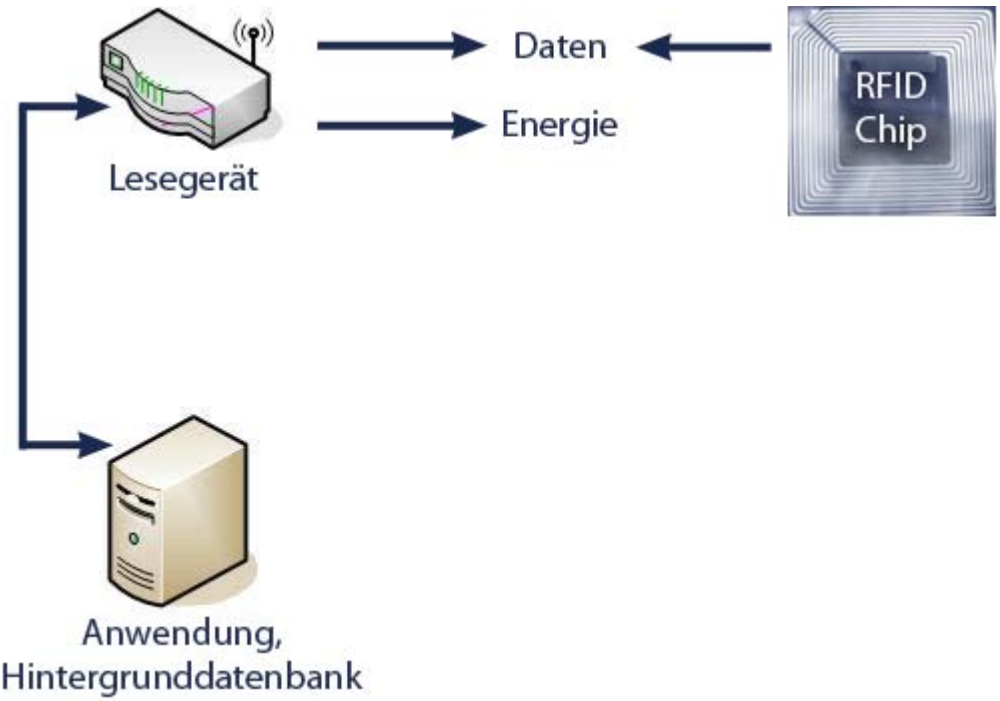


Abbildung 8: Bestandteile eines RFID-Systems

RFID-Chips lassen sich differenzieren nach der Art der Energieversorgung, dem verwendeten Frequenzbereich und damit verbunden der Reichweite und der Art der Datenübertragung sowie den Leistungsmerkmalen der in den Transpondern verbauten Chips.

Bezüglich der Energieversorgung werden aktive und passive Transponder unterschieden. Während aktive Transponder über eine eigene Energiequelle verfügen und von sich aus Signale aussenden können, beziehen passive Transponder die zum Betrieb erforderliche Energie aus den magnetischen, elektrischen oder elektromagnetischen Feldern, die von den Sende-/Empfangsgeräten abgestrahlt werden. Zur Kommunikation mit den Lesegeräten wird z.B. eine empfangene elektromagnetische Welle vom Transponder moduliert bzw. nicht moduliert, was den Werten „0“ und „1“ im digitalen Datenaustausch entspricht. Diese Veränderung kann vom Lesegerät wahrgenommen und entsprechend interpretiert werden.

Der verwendete Frequenzbereich ist maßgeblich für Bauform der Transponder, da unterschiedliche Frequenzen unterschiedlich große Antennen benötigen, sowie der möglichen Reichweite für eine Kommunikation mit den Lesegeräten. Exemplarisch[451] angeführt sei der Unterschied zwischen Transpondern, die im Hochfrequenzbereich (HF, z.B. bei 13,56 MHz) bzw. im Ultrahochfrequenzbereich (UHF, z.B. 2,4 GHz) arbeiten, da diese die größte Verbreitung haben und für den Einsatz im Endkundenmarkt vorgesehen werden. Während UHF-Transponder mit relativ kleinen Antennen auskommen und sich leicht kapseln lassen, sind HF-Transponder auf vergleichsweise großflächige

[451] Für eine umfassende technische Darstellung der RFID-Technik siehe [Finkenzeller 2006].

Antennen angewiesen. Aus den verwendeten Frequenzen ergeben sich auch unterschiedliche Anfälligkeiten für Störfaktoren. Während die Kommunikation von und mit HF-Transpondern durch Metall eingeschränkt werden kann, sind UHF-Transponder vornehmlich durch Flüssigkeiten betroffen, da 2,4 GHz der Eigenschwingfrequenz von Wassermolekülen entspricht (ein Effekt, den sich z.B. Mikrowellenherde zu Nutze machen). Ferner gelten für unterschiedliche Frequenzbereiche unterschiedliche maximale Emissionswerte und damit maximale Feldstärken für die Lesegeräte. Diese Werte können je nach Land unterschiedlich festgelegt sein, so dass die gleichen Systeme in unterschiedlichen Ländern für bestimmte Einsatzzwecke unterschiedlich gut geeignet sein können.

Das Spektrum der Leistungsmerkmale der in den Transpondern verbauten Chips beginnt bei 1-Bit-Diebstahlsicherungen (Information: „RFID-Chip ist vorhanden“) und Read-Only-Chips, die ihre fest eingebrannte Seriennummer ausgeben. Eine Vielzahl von Produkten wird im Bereich der Transponder mit (wieder-)beschreibbaren Datenspeichern angeboten, die auch einfache Kommandos ausführen können und sich über den als Adresse verwendeten Identifikator gezielt ansprechen lassen. Es existieren in diesem Bereich auch Transponder, die grundlegende kryptographische Funktionen unterstützen, in der Regel aber nur minimalen Schutz gegen Angriffe bieten. Hochklassige Transponder verfügen über Mikroprozessoren zur Datenverarbeitung und ggf. sogar kryptographische Koprozessoren, mit denen sich komplexere Mechanismen zur Authentifizierung und Verschlüsselung realisieren lassen. Zur Beurteilung der Sicherheit[452] von RFID-Systemen sind stets das gesamte System sowie das Einsatzumfeld zu betrachten.

4.4.2 Typische Anwendungsfälle

Ein RFID-System zur Objektidentifikation besitzt die folgenden Eigenschaften:

- Elektronische Identifikation: Das System ermöglicht eine eindeutige Kennzeichnung von „getaggten“[453] Objekten oder Personen durch elektronisch gespeicherte Daten.
- Kontaktlose Datenübertragung: Die Daten können zur Identifikation des Objekts drahtlos über einen Funkfrequenzkanal ausgelesen werden.
- Senden auf Abruf (*„on call“*): Ein gekennzeichnetes Objekt sendet seine Daten dann, wenn ein dafür vorgesehenes Lesegerät diesen Vorgang initiiert.

Nachfolgend werden zunächst typische Anwendungsfälle von RFID-Systemen dargestellt. Danach wird ausgeführt, wie RFID die Verkettung von Daten ermöglicht und erleichtert. Schließlich wird aufgezeigt, auf welcher Rechtsgrundlage dies geschieht bzw. geschehen darf und wie es um die Transparenz des Einsatzes von RFID für den Verbraucher bestellt ist[454].

Die Geschichte des Einsatzes von RFID reicht zurück bis in den Zweiten Weltkrieg, als Großbritannien Transponder einsetzte, um seine von Kampfeinsätzen zurückkehrenden Flugzeuge mit Hilfe von Radarsystemen zu identifizieren und sie dadurch von feindlichen Flugzeugen zu unterscheiden (Freund-Feind-Erkennung) [Garfinkel/Rosenberg 2005]. Heute findet auch in weiten Bereichen der Zivilgesellschaft ein Einsatz von RFID statt. In ihrem Alltag stoßen Bürger zunehmend auf RFID-Systeme, ohne sich dessen im Einzelnen immer bewusst zu sein.

4.4.2.1 Luftfahrt

In der Luftfahrt kann RFID zur Prozessoptimierung eingesetzt werden. Sowohl bei der Passagierabfertigung als auch bei der Gepäckabfertigung und Gepäcksortierung ist RFID einsetzbar.[455] Im Rahmen der Passagierabfertigung wird an das Ausstellen RFID-fähiger Tickets gedacht, um durch die Verfolgung von Passagierströmen die Sicherheit im Flughafen zu erhöhen und Prozesse besser planbar zu machen. Dem Flugpassagier könnten zusätzlich über sein RFID-Flugticket Richtungs-

[452] [BSI 2004], abrufbar unter http://www.bsi.de/fachthem/rfid/studie.htm (letzter Zugriff im Oktober 2007).
[453] D.h. mit einem RFID-Tag versehen.
[454] Umfassend erörtert werden die hiermit verbundenen Fragestellungen aus europäischer Sicht im Arbeitspapier der Art. 29-Datenschutzgruppe „Datenschutzfragen im Zusammenhang mit der RFID-Technik“ [Art. 29-Datenschutzgruppe 2005] sowie bei [EICAR 2006].

informationen im Flughafen sowie spezielle Informationen für den jeweiligen Flug angeboten werden und er könnte im Falle einer Verspätung ausfindig gemacht werden. Im Gepäckprozess kann jedes Gepäckstück mit einem RFID-Transponder versehen und dann in allen Bereichen der Abfertigung durch Lesegeräte lokalisiert und verfolgt werden.

4.4.2.2 Gesundheitswesen

Im Gesundheitswesen wird RFID[456] bereits von der Arzneimittelindustrie verwendet, um Arzneimittel zu lokalisieren und Fälschungen oder Verluste durch Diebstahl während des Transports zu verhindern. In Krankenhäusern kann RFID zur Prozesssteuerung genutzt werden, um Ressourcen zu verteilen, die Warenlogistik von Krankenhäusern zu optimieren (siehe Abschnitt 4.4.2.4) oder Dokumentationsprozesse zu automatisieren. Die Lokalisierung und Nachverfolgung von Personen, Medikamenten, Materialien und Geräten wird ebenfalls in Kliniken eingesetzt. Bei der Medikation wird erwogen, RFID zur personalisierten Medikation einzusetzen, um dadurch die Irrtümer bei der Medikamentenvergabe auszuschließen und so die Patientensicherheit zu erhöhen. Durch RFID-Systeme ist es in Krankenhäusern zudem möglich, Angaben über die Medikamentengabe in die elektronische Patientenakte zu übertragen. Auch möglich ist, RFID zur Messdatenüberwachung zu nutzen und einen Alarm auslösen zu lassen, wenn ein Grenzwert überschritten wird.

4.4.2.3 Verkehr

Auch für verkehrstechnische Anwendungen wird RFID eingesetzt. Neben Autoschlüsseln, die mit RFID ausgestattet für die Authentifizierung beim Zugang genutzt werden, gibt es bereits Länder, die RFID-gestützte Verkehrsüberwachungssysteme[457] einsetzen. Dabei werden mit einem RFID-Chip versehene Plaketten an der Windschutzscheibe oder RFID-Nummernschilder (*E-Plates*) von stationären oder mobilen Lesegeräten ausgelesen. Auch für Maut-Systeme[458] lässt sich RFID nutzen.

4.4.2.4 Einzelhandel

Im Einzelhandel und in der Warenwirtschaft wird RFID schon seit vielen Jahren eingesetzt. Um den Weg der Ware in der Wertschöpfungskette nachvollziehen zu können oder um Just-in-Time-Anlieferungen zu koordinieren, werden Gegenstände im Handel mit RFID-Chips versehen. Auch das Bestellwesen kann über RFID-Etiketten optimiert und Lagerbestände durch automatisierte Bestellvorgänge verringert werden. Für den Einzelhandel ermöglicht RFID zudem eine permanente automatische Inventur sowie eine Kontrolle der Mindesthaltbarkeitsdaten von verderblichen Waren. Denkbar ist auch ein Einsatz von RFID für die Prüfung von Gewährleistung- oder Garantiepflichten bei Kaufgegenständen.

---

455 Einen Überblick über den Einsatz von RFID in der Luftfahrt gibt Airliners, „RFID in der Luftfahrt“, abrufbar unter http://www.airliners.de/safety/sonderthemen/RFID/luftfahrt.php (letzter Zugriff im Oktober 2007). Vgl. auch Siemens, „Mehr Sicherheit in der Luftfahrt“, abrufbar unter http://www.automation.siemens.com/rfid/html_00/branchen_luftfahrt.htm (letzter Zugriff im Oktober 2007). Siemens unterhält ein Innovations- und Erprobungszentrum für Infrastrukturprojekte in Flughäfen, wo auch der Einsatz von RFID in der Luftfahrtbranche getestet wird. Vgl. http://www.airliners.de/safety/nachrichten/artikelseite.php?articleid=7019 (letzter Zugriff im Oktober 2007).

456 Einen Überblick über den möglichen Einsatz von RFID im Gesundheitswesen bietet [Info-RFID 2006].

457 So beispielsweise Bermuda und Malaysia. Vergleiche Meldungen bei heise online: „Bermuda startet RFID-gestütztes Verkehrsüberwachungssystem“, 09.05.2007, abrufbar unter http://www.heise.de/newsticker/meldung/89504 (letzter Zugriff im Oktober 2007) und „RFID-Nummernschilder: Ein Aprilscherz wird Realität“, 13.12.2006, abrufbar unter http://www.heise.de/newsticker/meldung/82486/ (letzter Zugriff im Oktober 2007). Auch die Vereinigten Arabischen Emirate und Großbritannien haben bereits RFID-Nummernschilder getestet: http://www.heise.de/newsticker/meldung/62666/ (letzter Zugriff im Oktober 2007) und http://www.heise.de/newsticker/meldung/58623/ (letzter Zugriff im Oktober 2007).

458 Für München: http://www.heise.de/newsticker/meldung/47583/ (letzter Zugriff im Oktober 2007). Für Großbritannien: http://www.sun.com/br/0504_ezine/gov_traffic.html (letzter Zugriff im Oktober 2007).

4.4.2.5 Sicherheit und Zugangskontrolle

Ein weiterer Anwendungsbereich für RFID besteht im Rahmen von Zugangskontrollen und Sicherheitsanwendungen. Zur Zutrittskontrolle werden zumeist Schleusensysteme eingesetzt oder in den Türrahmen wird eine Zugangskontrolle installiert. Zum Zugang Berechtigte verfügen über einen RFID-Transponder, der häufig auf einer Chipkarte aufgebracht ist.

RFID kann auch in Wegfahrsperren von Autos oder zur Verfolgung wertvoller Gegenstände Anwendung finden. EU-weit wird RFID mittlerweile für biometrische Reisepässe eingesetzt. Auf dem in den Pass eingearbeiteten RFID-Chip sind ein digitales Gesichtsbild und zukünftig auch ein digitaler Fingerabdruck gespeichert. Diese werden durch Lesegeräte bei Grenzübertritten außerhalb des Schengenraums ausgelesen.

4.4.3 Verkettung von Daten

Jeder RFID-Chip enthält einen eindeutigen Bezeichner (Identifier), mit dem sich die getaggten Objekte oder Personen eindeutig identifizieren lassen. RFID-Chips werden dabei überwiegend in Objekte eingebettet. Nur selten werden RFID-Chips Personen direkt implantiert.[459] Ein direktes *„Chippen“* von Personen kann auch über Armbänder mit RFID-Transponder oder andere sicher mit einer Person zu verbindende Gegenstände geschehen. Wenn in einem Hintergrundsystem einer bestimmten Person ein eindeutiger Bezeichner zugeordnet ist, kann der Betroffene direkt durch das RFID-System identifiziert werden.

Nicht alle in RFID-Systemen verarbeiteten Daten sind personenbezogen und lassen sich mit anderen Daten über Personen verknüpfen. In der Warenwirtschaft, einem Hauptanwendungsfall der RFID-Technologie, sind einzelne Waren oder ganze Paletten mit RIFD-Etikett versehen. Eine Zuordnung von RFID-getaggten Objekten zu bestimmten oder bestimmbaren Personen ist prinzipiell möglich, spätestens wenn die Person identifiziert ist oder sich beispielsweise durch einen Zugriff auf das Zeiterfassungssystem oder den Dispositionsplan für eine Fahrflotte bestimmen lässt. Ein Verketten von mittels RFID erhobenen Daten mit personenbezogenen Daten ist insbesondere im Einzelhandel und im Gesundheitsbereich denkbar und kann nicht technisch wirksam ausgeschlossen werden.

Wenn ein Käufer über den Einsatz von EC-Karten, Kundenbindungskarten oder auch durch den Einsatz von Videoüberwachung in Einkaufsräumen bestimmt oder bestimmbar ist, besteht die Möglichkeit über einen zeitlichen Abgleich von Einkaufsvorgängen mit Personen die Nummer von RFID-Produkten zu verketten. Eine solche Verknüpfung in einer Kundendatei des Händlers kann zu Garantiezwecken erfolgen. Darüber hinaus besteht an der Erstellung von präzisen Kundenprofilen ein wirtschaftliches Interesse, um gezieltere Werbeansprachen angelehnt an die persönlichen Präferenzen von Kunden vornehmen zu können. Nicht nur im Kassenbereich hinsichtlich tatsächlich getätigter Einkäufe, sondern auch in den Verkaufsräumen ist eine Verkettung von Informationen über das Verhalten von einzelnen Kunden denkbar. Gibt ein Unternehmen eine mit RFID-Technologie versehene Kundenkarte aus, kann über im Verkaufsraum platzierte Lesegeräte die Aufenthaltsdauer des Kunden in einzelnen Abteilungen des Unternehmens erfasst werden, um auch diese Informationen für Rückschlüsse auf persönliche Präferenzen des Kunden zu nutzen. Zwar ist auch heute im Einzelhandel die Erstellung von Kundenprofilen mittels Kundenbindungssystemen weit verbreitet; allerdings muss der Kunde insoweit für jeden Einkauf bewusst die Entscheidung treffen, die Kundenkarte beim Bezahlvorgang einzusetzen und dadurch Rabattpunkte zu sammeln.

Über den Einkaufsvorgang hinaus ist auch ein Wiedererkennen einzelner Personen, deren Konsumverhalten sowie ggf. die Identifizierung von Beziehungen zwischen verschiedenen Personen auch dann erfassbar und auswertbar, wenn die Namen der betroffenen Personen nicht in Erfahrung gebracht werden.[460]

---

[459] Das bekannteste Anwendungsbeispiel hierfür ist der VeriChip der Verichip Corporation. http://www.verichipcorp.com/content/company/rfidtags#implantable (letzter Zugriff im Oktober 2007).

[460] Vgl. [Hansen/Meissner 2007], die die Erkennung und das Verfolgen einer Person anhand des Electronic Product Codes auf von ihr herum getragenen RFID-Tags aufzeigen und dies mit Methoden biometrischer Erkennung in Beziehung setzen.

In der Warenwirtschaft eingesetzte RFID-Etiketten[461] verfügen, um sie kostengünstig und damit wirtschaftlich massenhaft einsetzen zu können, nicht über den Anschaffungspreis erhöhende Verschlüsselungsfunktionen oder so genannte „Kill-Funktionen“, die eine Datenübertragung in der Zukunft unterbinden. Nur bei sicheren RFID-Systemen muss das Lesegerät seine Berechtigung gegenüber dem RFID-Chip nachweisen. Solche Sicherheitsmaßnahmen werden derzeit teilweise im Bereich der Zugangskontrolle eingesetzt und auch in der RFID-Infrastruktur des biometrischen Reisepasses.[462] In der Warenwirtschaft sind sichere RFID-Systeme eine Ausnahme.

4.4.4 Rechtliche Grundlagen

Eine Datenverarbeitung im nichtöffentlichen Bereich kann grundsätzlich auf eine Einwilligung des Betroffenen oder die §§ 27 ff. BDSG gestützt werden. In der Praxis muss daher für jede Erhebung, Verarbeitung oder Nutzung und damit auch für die Verkettung personenbezogener Daten mit Hilfe von RFID-Systemen eine Einwilligung des Betroffenen oder eine Rechtsvorschrift vorliegen, die die Verarbeitung erlaubt. Auch wenn das Auslesen technisch bei nicht gesicherten RFID-Systemen möglich ist, sobald ein Transponder in die Reichweite eines Lesegeräts kommt, ist ein Auslesen nicht ohne Rechtsgrundlage zulässig. Werden RFID-Chipkarten eingesetzt, ist zusätzlich auch § 6c BDSG einschlägig. Wichtig für ein RFID-System ist ferner der Grundsatz der datenvermeidenden und datensparsamen Gestaltung, vgl. § 3a S. 1 BDSG und der Einsatz von Anonymisierung und Pseudonymisierung, wenn dies mit angemessenem Aufwand möglich ist, § 3a S. 2 BDSG.

Der Zweck der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten muss vorher konkret festgelegt sein. Sollen personenbezogene Daten für einen anderen Zweck genutzt werden (Zweckänderung), muss auch für diese zweckändernde Nutzung eine Rechtsgrundlage bestehen. Sollen in einem anderen Zusammenhang gesammelte Daten in einem Nutzerprofil verkettet werden, ist eine Einwilligung des Betroffenen erforderlich.

Auch für RFID-Systeme sind durch die verarbeitende Stelle die Regelungen in § 9 BDSG zu technischen und organisatorischen Maßnahmen zu beachten, die erforderlich sind, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen.

Während verschiedene Stellen[463] die Einführung spezieller Rechtsvorschriften für den Einsatz von RFID gefordert haben, hat auch der Bundestag in einer Entschließung die Bundesregierung aufgefordert, über ihre Aktivitäten und Planungen und einen möglichen gesetzgeberischen Handlungsbedarf zu berichten[464]. Auf europäischer Ebene hat es die Europäische Kommission im April 2007 vorläufig abgelehnt, eine gesetzliche Regelung zu schaffen[465]. Zuvor hatte die Kommission eine öffentliche Konsultation zum Einsatz von RFID-Systemen durchgeführt.

4.4.5 Folgen für den Betroffenen

Da RFID das kontaktlose, unbemerkte Auslesen von Daten aus unter Umständen beträchtlicher Entfernung ermöglicht, besteht ein immanentes Transparenzdefizit bei Auslese- und Datenübermittlungsvorgängen. Eine Kenntnis von einzelnen Datenübermittlungen fehlt dem Betroffenen, falls keine technischen Mittel (Hinweiston, Hinweislicht, Displayanzeige, Aufdruck auf den Kassenzettel, etc.) aus Transparenzgründen eingesetzt werden. Die Miniaturisierung von RFID-Systemen und die kosten-

[461] Zum Electronic Product Code (EPC) und der Klassifizierung des Auto-ID-Centers: [BSI 2004].

[462] Kritisch zur Sicherheit der RFID-Infrastruktur des ePasses: [Meints/Hansen 2006].

[463] Bereits 2004 der Bundesbeauftragte für Datenschutz und Informationsfreiheit: http://www.heise.de/newsticker/meldung/47414/ (letzter Zugriff im Oktober 2007). Ebenso: 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. Oktober 2006 „Verbindliche Regelungen für den Einsatz von RFID-Technologien“, abrufbar unter http://www.sachsen-anhalt.de/LPSA/index.php?id=20563/ (letzter Zugriff im Oktober 2007).

[464] Vgl. Bundestags Drucksache 16/4882. Noch im Oktober 2006 hatte sich die Große Koalition gegen eine RFID-Regulierung ausgesprochen: http://www.heise.de/newsticker/meldung/80167/ (letzter Zugriff im Oktober 2007).

[465] Heise online vom 15.03.2007: „EU-Kommission will gemeinsame RFID-Strategie“. http://www.heise.de/newsticker/meldung/86793/ (letzter Zugriff im Oktober 2007). Vgl. auch http://www.zdnet.de/news/tkomm/0,39023151,39153277,00.htm (letzter Zugriff im Oktober 2007).

günstigen Komponenten ermöglichen zudem einen massenhaften Einsatz. RFID ist eine zentrale Technologie der allgegenwärtigen Datenverarbeitung („Ubiquitous Computing“).[466] Dabei werden Chips in Gegenstände unserer Umwelt eingebettet und Computer dadurch allgegenwärtig. Durch den Einsatz von Hintergrundsystemen wird die Verarbeitung und Auswertung übermittelter Daten durchgeführt. Dabei ist, wenn bereits keine Transparenz hinsichtlich der Datenübermittlung besteht, für den Betroffenen kaum nachvollziehbar, dass eine Auswertung von Daten in Hintergrundsystemen stattfindet. Durch eine Vernetzung solcher Hintergrundsysteme können Informationen über einzelne Personen aus verschiedenen Quellen oder Einsatzbereichen von RFID verkettet werden.

4.4.6 Betroffenenrechte

Auch Transparenz unterstützende Informations- und Unterrichtungspflichten sind im Rahmen eines Einsatzes von RFID-Systemen einschlägig. Der Betroffene ist gemäß § 33 BDSG bei der erstmaligen Speicherung seiner Daten über die Speicherung, die Art der Speicherung, die Zweckbestimmung der Erhebung und die Identität der verantwortlichen Stelle zu informieren. So muss die RFID ausgebende Stelle nach § 4 Abs. 3 BDSG den Betroffenen bei der Erhebung seiner Daten informieren[467] über

- die Identität der verarbeitenden Stelle,
- die Zweckbestimmung der Erhebung, Datenverarbeitung und Nutzung,
- die Kategorien von Empfängern, sofern der Betroffene nicht mit einer Übermittlung an diese rechnen muss,
- Lokalisierung des RFID-Chips,
- personenbezogene Inhalte des RFID-Chips sowie
- Möglichkeiten der Deaktivierung und Löschung.

Wenn es sich bei dem System um eine RFID-Chipkarte handelt, ist nach § 6c BDSG auch zu informieren über

- die Identität und Anschrift der ausgebenden Stelle und der Stelle, die auf das Medium Verarbeitungsverfahren aufbringt,
- die Funktionsweise des Mediums,
- die Rechte des Betroffenen auf Auskunft und Korrektur sowie
- Maßnahmen, die bei Verlust oder Zerstörung zu treffen sind.

Ferner steht dem Betroffenen der Auskunftsanspruch aus § 34 BDSG gegen die verantwortliche Stelle zu. Eine Pflicht zur Löschung von personenbezogenen Daten besteht, wenn die Datenerhebung und -speicherung unzulässig ist, vgl. § 35 Abs. 2 Nr. 1 BDSG. Auch wenn eine Speicherung der Daten nicht mehr zur Erfüllung des festgelegten Zwecks erforderlich ist, müssen die Daten gelöscht werden, vgl. § 35 Abs. 2 Nr. 3 BDSG.

4.4.7 Fazit

Die Durchdringung des Alltags mit RFID-Systemen wird zunehmen. Aufgrund der systemimmanenten Transparenzdefizite ist von verantwortlichen Stellen besonderes Augenmerk auf eine datenschutzgerechte Implementierung des Systems zu richten. Durch den Einsatz von Möglichkeiten zur Deaktivierung von RFID-Chips könnte das Recht auf informationelle Selbstbestimmung gestärkt werden. Durch Hintergrundsysteme bieten RFID-Systeme vielfältige Möglichkeiten zur für den Betroffenen im Einzelfall möglicherweise unbewussten Verkettung von Daten mit Personenbezug.

[466] Ausführlich dazu: [TAUCIS 2006].
[467] [EICAR 2006].

4.5 Basiskonzepte

In diesem Abschnitt werden grundlegende Konzepte dargestellt, die zur Kontrolle der Verkettbarkeit der in Kommunikationsvorgängen anfallenden Daten verwendet werden können.

Entsprechend den oben vorgestellten grundlegenden Schutzzielen können die Basiskonzepte in drei Kategorien eingeteilt werden:

1. *Konzepte, die die Vertraulichkeit sichern:* Es wird davon ausgegangen, dass grundlegende Konzepte der vertraulichen Übertragung von Nachrichteninhalten im Wesentlichen bekannt sind (Verschlüsselungstechniken), so dass in dieser Arbeit nicht speziell darauf eingegangen werden muss. Es sollen hier vielmehr erweiterte Konzepte vorgestellt werden, die zusätzlich den Schutz der Kommunikationsumstände (d.h. Anonymität des Senders bzw. Empfängers einer Nachricht) ermöglichen. Solche Konzepte werden in Abschnitt 4.5.1 vorgestellt.
2. *Konzepte, die zur Sicherung der Authentizität und Zurechenbarkeit von übertragenen Daten beitragen:* Hierzu gehören herkömmliche digitale Signaturen, die die Authentizität und Zurechenbarkeit von Daten sichern ebenso wie Reputationssysteme, die zur Sicherung der Authentizität bzw. Verlässlichkeit von Akteuren (Nutzern, Geräten) beitragen. Diese Konzepte werden in Abschnitt 4.5.2 vorgestellt.
3. *Konzepte, die Authentizität und Zurechenbarkeit sichern, aber dabei gleichzeitig Vertraulichkeit gewährleisten:* Hierzu gehört das grundlegende Konzept des Pseudonyms, sowie Techniken, die Authentizität und Zurechenbarkeit von unter Pseudonym ausgetauschten Daten für verschiedene Zwecke ermöglichen. Abschnitt 4.5.3 gibt einen Überblick über derartige Konzepte.

4.5.1 Sicherung der Vertraulichkeit der Kommunikationsumstände

Solche Techniken werden oft als Anonymisierungstechniken bzw. Anonymisierungsdienste bezeichnet. Mit dem Proxy-Konzept wird zunächst eine einfach umzusetzende, aber nur gegen schwache Angreifer sichere Variante beschrieben.

Als ein auch gegen mächtigere Angreifer unter bestimmten Bedingungen sicheres Konzept folgt zunächst das Mix-Konzept, dessen praktische Umsetzung an zwei Beispielen erläutert wird. Weiterhin wird mit dem DC-Netz das stärkste derzeit bekannte Anonymisierungskonzept vorgestellt.

4.5.1.1 Proxy-Konzept

Ein Proxy (zu Deutsch: Stellvertreter) kann zwischen den Browser eines Internetnutzers und die von ihm angefragten Webserver geschaltet werden. Er hat die Aufgabe, angefragte Webseiten anstelle des Nutzers abzurufen. Manche Institutionen erlauben ihren Mitgliedern (z.B. Mitarbeiter und Studierende von Universitäten) den Internetzugriff sogar nur über so genannte Zwangs-Proxies. Es ist dadurch möglich, bestimmte unerwünschte Webserver für die Nutzer, die über einen solchen Zwangs-Proxy auf das Internet zugreifen, zu sperren. Beispielsweise erlauben einige Staaten ihren Bürgern nur den Zugriff auf einen Teil des Internets. Gegenüber einem Browser (Client) erscheint der Proxy als Webserver, während er gegenüber einem Webserver einen Client darstellt.

Ein Anonymisierungs-Proxy nutzt das obige Prinzip aus. Der Webserver oder auch ein hinter dem Anonymisierungs-Proxy befindlicher Lauscher erfährt nicht, wer eigentlich auf die Webseite zugreifen wollte, da der Anonymisierungs-Proxy stellvertretend als Anfragender auftritt.

Es existieren mehrere Anbieter von Anonymisierungs-Proxies im Internet, z.B. Anonymizer[468] oder Rewebber[469], die sich durch den Vorteil auszeichnen, dass auf dem eigenen Rechner keine zusätzlichen Programme installiert werden müssen.

[468] http://www.anonymizer.com/ (letzter Zugriff im Oktober 2007).
[469] Ehemals unter http://www.rewebber.com/.

Einige Tools für den Bereich Sicherheit, z.B. Steganos[470], bieten anonymes Websurfen, indem sie Webseitenaufrufe über allgemein zugängliche, so genannte „offene“ Proxies umleiten, die damit als Anonymisierungs-Proxies fungieren (mitunter unbeabsichtigt durch die Betreiber dieser Proxies). Um eine hohe Verfügbarkeit zu erreichen, verwalten diese Programme ganze Listen der verwendbaren Proxies, die während des Surfens regelmäßig gewechselt werden.

Bei allen obigen Realisierungsarten ruft der Anonymisierung-Proxy dann die angefragte Webseite in seinem eigenen Namen auf, so als wäre er der Nutzer. Anonymisierungs-Proxies realisieren damit zwar Anonymität des Internetnutzers gegenüber dem Webserver und, falls verschlüsselt wird, auch vor dem eigenen Internet-Service-Provider, nicht jedoch gegenüber dem Betreiber des Anonymisierungs-Proxies. Dieser kann die dem Nutzer zugeordnete IP-Adresse natürlich mit der angefragten Webseite verknüpfen. Es kann daher wohl nur eine Frage der Zeit sein, bis potenzielle Datensammler selbst Anonymisierungs-Proxies betreiben.

Häufig wird für die Programme, die anonymes Websurfen über freie Proxies realisieren, damit geworben, dass die Verwendung mehrerer Proxies für die Anonymisierung vorteilhaft sei. Da aber zu einem Zeitpunkt immer nur ein Proxy verwendet wird, ist dem jeweils verwendeten Proxy die Zuordnung zwischen IP-Adresse und angefragter Webseite bekannt.

Anonymisierungs-Proxies realisieren auch keine Unbeobachtbarkeit gegenüber externen Beobachtern, die Leitungen überwachen und damit (zumindest theoretisch) genau wissen, zu welchem Zeitpunkt die Anfrage einer Webseite im Anonymisierungs-Proxy eingegangen ist. Da der Proxy diese sofort bearbeitet, kann ein „Big Brother“ die Anfrage und die zugehörige angefragte Webseite leicht miteinander verketten. Gegen diese Beobachtung hilft selbst Verschlüsselung nicht, da die zeitliche Zusammengehörigkeit nach wie vor beobachtbar bleibt.

Eine Verschlüsselung zwischen Nutzer und Proxy sowie zwischen Proxy und Zielserver verbirgt zwar vor fremden Blicken, für welche Inhalte (z.B. welche Webseiten) sich der Nutzer interessiert. Die Kommunikationsbeziehung als solche, d.h., welcher Webserver aufgerufen wird, ist dagegen trotzdem beobachtbar.

4.5.1.2 Mix-Konzept

Das Verfahren der umcodierenden Mixe verwirklicht Unverkettbarkeit zwischen Sender und Empfänger einer Nachricht gegenüber Außenstehenden und auch ggf. gegenüber einander [Chaum 1981], [Chaum 1984].

Bei diesem von David Chaum 1981 für elektronische Post vorgeschlagenen Verfahren werden Nachrichten von ihren Sendern nicht notwendigerweise auf dem kürzesten Weg zu ihren Empfängern geschickt, sondern über mehrere möglichst bezüglich ihres Entwurfs, ihrer Herstellung ([Pfitzmann 1986, S. 356]) und ihres Betreibers ([Chaum 1981], [Chaum 1984, S. 99]) unabhängige sowie Nachrichten derselben Länge puffernde, umcodierende und umsortierende Zwischenstationen, so genannte Mixe, geleitet. Jeder Mix codiert Nachrichten derselben Länge um, d.h. ent- oder verschlüsselt sie unter Verwendung eines Konzelationssystems, so dass ihre Wege über ihre Länge und Codierung, was zusammen genommen ihr äußeres Erscheinungsbild ergibt, nicht verfolgt werden können.

Damit dieses Verfolgen des Weges auch über zeitliche oder räumliche Zusammenhänge nicht möglich ist, muss jeder Mix jeweils mehrere Nachrichten derselben Länge von genügend vielen unterschiedlichen Absendern abwarten (oder ggf. auch selbst erzeugen oder von Teilnehmerstationen erzeugen lassen – sofern nichts Nützliches zu senden ist, eben bedeutungslose Nachrichten, die von der Teilnehmerstation des Empfängers oder bei geeigneter Verschlüsselungsstruktur und Adressierung bereits von einem der folgenden Mixe ignoriert werden), sie dazu puffern und nach der Umcodierung umsortiert, d.h. in anderer zeitlicher Reihenfolge bzw. auf anderen Leitungen, ausgeben. Eine geeignete Reihenfolge ist etwa die alphabetische Ordnung der umcodierten Nachrichten. Solch eine von vornherein vorgegebene Reihenfolge ist besser als eine zufällige, da so der verborgene Kanal (engl.: „covert / hidden channel“) der „zufälligen“ Reihenfolge für ein eventuell im jeweiligen Mix vorhandenes Trojanisches Pferd geschlossen wird. Da auch die Anzahl der jeweils

[470] http://www.steganos.com/ (letzter Zugriff im Oktober 2007).

gleichzeitig zu mixenden Nachrichten sowie die Zeitverhältnisse exakt vorgegeben werden können und dem Mix das Erzeugen von Nachrichten verboten werden kann, braucht der Mix keinerlei Handlungsspielraum und damit braucht keinerlei Möglichkeit zu bestehen, über die ein eventuell im Mix vorhandenes Trojanisches Pferd einem nicht empfangsberechtigten Empfänger verborgen Information zukommen lassen kann (vgl. [Popek/Kline 1978], [Denning 1982, S. 281]).

Die zum Zwecke des Verbergens zeitlicher oder räumlicher Zusammenhänge zusammen gemixten, d.h. zusammen gepufferten (oder erzeugten), umcodierten und umsortiert (beispielsweise in alphabetischer Reihenfolge) ausgegebenen Nachrichten derselben Länge werden als ein Schub (engl.: „batch“ [Chaum 1981, S. 85]) bezeichnet.

Zusätzlich zum Puffern, Umcodieren und Umsortieren von Nachrichten derselben Länge muss jeder Mix darauf achten, dass jede Nachricht nur einmal gemixt wird – oder anders herum gesagt: Nachrichtenwiederholungen ignoriert werden. Eine Eingabe-Nachricht stellt genau dann eine Nachrichtenwiederholung dar, wenn sie schon einmal bearbeitet wurde und die jeweils zugehörigen Ausgabe-Nachrichten von Unbeteiligten verkettbar (beispielsweise gleich) wären[471].

Wird eine Nachricht innerhalb eines Schubes mehrfach bearbeitet, so entstehen über die Häufigkeiten der Eingabe- und Ausgabe-Nachrichten dieses Schubes unerwünschte Entsprechungen: einer Eingabe-Nachricht, die *n*-mal auftritt, entspricht eine Ausgabe-Nachricht, die ebenfalls *n*-mal auftritt. Treten alle Eingabe-Nachrichten eines Schubes verschieden häufig auf, so schützt das Umcodieren dieses Schubes also überhaupt nicht.

Wird eine Nachricht in mehreren Schüben bearbeitet, so können zwischen diesen Schüben nichtleere Durchschnitte (und Differenzen) gebildet werden, indem man jeweils den Durchschnitt (die Differenz) der Eingabe- und Ausgabe-Nachrichten berechnet, wobei beim Durchschnitt (bei der Differenz) von letzteren im allgemeinen Fall statt Gleichheit Verkettbarkeit geprüft wird. Natürlich können diese beiden Operationen wiederum auf beliebige Operationsergebnisse angewendet werden. Bei Nachrichten, die in einem Durchschnitt (einer Differenz) der Kardinalität 1 liegen, ist die Entsprechung zwischen Eingabe- und Ausgabe-Nachricht klar – bezüglich dieser Nachrichten stellt der Mix also keine Unverkettbarkeit her.

Die in diesem Abschnitt hergeleiteten und beschriebenen Grundfunktionen eines Mixes sind in Abbildung 9 dargestellt.

[471] Wann dies genau der Fall ist, hängt vom verwendeten Umcodierungsschema ab, auf das hier nicht näher eingegangen wird.

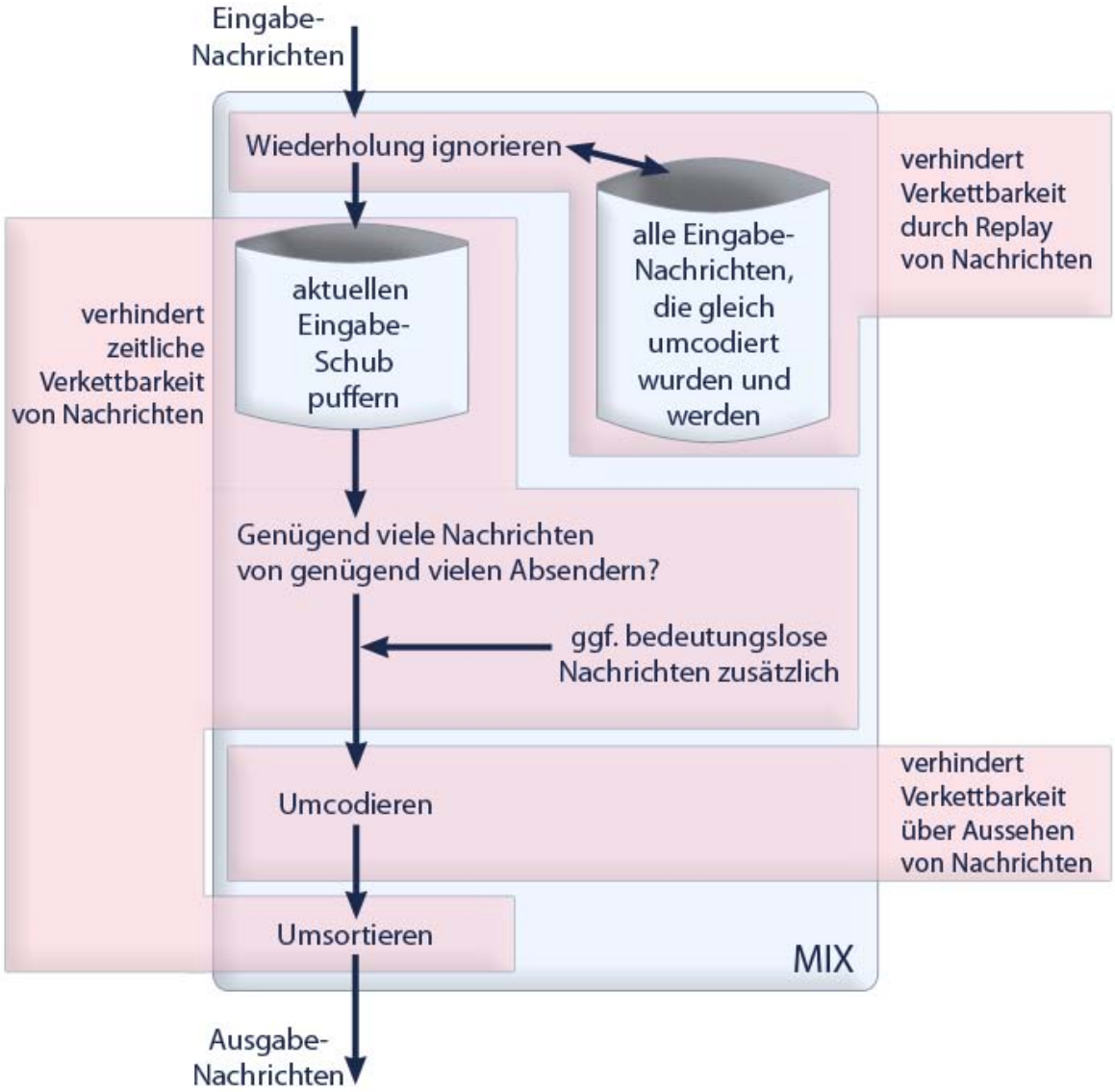


Abbildung 9: Grundfunktionen eines Mixes

Wandelt man das Mix-Verfahren wie erstmals in [Pfitzmann 1985, S. 25-29] beschrieben ab, so kann man anonyme Kanäle schalten, die Realzeitanforderungen genügen. Hierzu wird zum Kanalaufbau eine spezielle Nachricht nach dem oben beschriebenen Verfahren übertragen, die jedem gewählten Mix einen Schlüssel eines schnelleren symmetrischen Konzelationssystems übergibt, den dieser Mix von da an für die Entschlüsselung des Verkehrs auf diesem Kanal verwendet. Das Umcodieren bei Kanälen nützt natürlich nur dann etwas, wenn mindestens zwei Kanäle von gleicher Kapazität durch denselben Mix gleichzeitig auf- und abgebaut werden.

Um die Vertrauenswürdigkeit in ein Mix-basiertes Anonymisierungssystem zu erhöhen, werden in der Regel mehrere Mixe (die idealerweise von unterschiedlichen Organisationen bzw. Personen betrieben werden) hintereinander geschaltet. Dies ist sinnvoll, da sich der Weg einer Nachricht im Netz typischerweise nicht feststellen lässt, wenn nicht alle an der Weiterleitung beteiligten Mixe zusammenarbeiten. Bezüglich der Art und Weise der Zusammenschaltung von Mixen lassen sich einige grundsätzlich verschiedene Möglichkeiten unterscheiden, wobei die beiden Extrem durch ein so genanntes „freies Mixnetz“ auf der einen Seite und „Mixkaskaden“ (kurz: Kaskaden) auf der anderen Seite

gegeben sind. Dazwischen existiert eine Reihe von Abwandlungen, wie beispielsweise Mixnetze mit beschränkten Routen [Danezis 2003].

Jede dieser Verknüpfungsformen von Mixen hat ihre speziellen Vor- und Nachteile bezüglich Sicherheit, Skalierbarkeit, Praktikabilität, Performance, Effizienz etc. Ein entsprechender Vergleich und eine umfangreiche Diskussion der Thematik „Freies Mixnetz vs. Mixkaskaden“ lässt sich [Böhme et al. 2004] entnehmen – ein klarer „Sieger“ existiert demnach nicht.

4.5.1.2.1 Beispiel „AN.ON“

Beim Mix-basierten Anonymisierungsdienst AN.ON[472] mit der Client-Software JAP wurde als Verknüpfungsform der Mixe die Kaskade gewählt. Sie besitzt gegenüber dem Mixnetz eine geringere Komplexität, was zu einfacherer Analyse bezüglich Sicherheit und zu erwartetem geringeren Aufwand in der Implementierung führt. Es hat sich gezeigt, dass die freie Folge eine Reihe von Sicherheitsproblemen birgt, die bei Kaskaden nicht existieren [Berthold/Pfitzmann/Standke 2000]. Um Echtzeitkommunikation in Form von Websurfen zu realisieren, wurden Kanäle verwendet, die zuverlässige verbindungsorientierte Byteströme zwischen Sender und Empfänger zulassen. Durch die Verwendung eines Schlüsseltransportmechanismus (Verschlüsselung eines symmetrischen Schlüssels mittels RSA) kann ein symmetrisch verschlüsselter Kanal aufgebaut werden.

Der Anonymisierungsdienst bietet nur die Möglichkeit, Klassen von Proxies zu adressieren, d.h., ein Nutzer kann nur entscheiden, dass seine Daten z.B. an einen HTTP-Proxy geschickt werden sollen. Die Proxies sind für die weitere Verarbeitung der Daten gemäß dem jeweiligen Proxy-Protokoll zuständig. Ein Vorteil ist, dass die Verarbeitung des Proxy-Protokolls auf erprobte und ausgereifte Komponenten ausgelagert werden kann, die oft noch zusätzliche Funktionalität bieten (Zugriffskontrolle, Ressourcenbegrenzung, Caching etc.). Des Weiteren sind viele der nutzerseitig vorhandenen Anwendungen (beispielsweise Web-Browser) in der Lage, Proxies in die Kommunikationskette zwischen Client und Server einzubinden. Somit existiert eine weit verbreitet und einfach zu benutzende Möglichkeit der Anbindung des Anonymisierungsdienstes an die Anwendungen der Nutzer. Darüber hinaus stellt die vorgesehene Adressierungsmethode aus praktischer Sicht keine Einschränkung da, da Proxy-Protokolle (beispielsweise SOCKS [RFC 1928]) für „einfache“ TCP/IP-Verbindungen existieren.

Neben den Mix-Servern, die den grundlegenden Anonymisierungsdienst bilden, wird eine Client-Komponente benötigt. Diese muss auf den Endsystemen (z.B. Rechner der Nutzer) installiert sein. Sie ist für den Transfer der anonym zu übertragenden Daten zuständig und bereitet diese dem Protokoll des zugrundeliegenden Anonymisierungsdienstes gemäß auf. Diese Client-Komponente wird als JAP-Software bezeichnet.

Um die Benutzung des Anonymisierungsdienstes zu erleichtern und dem Nutzer eine Rückmeldung über sein aktuelles Schutzniveau zu geben, wurde ein dritter Bestandteil in das Gesamtsystem aufgenommen – der so genannte InfoService. Dieser ist mit einer Datenbank vergleichbar und hält abrufbar Informationen über die aktuell verfügbaren Mixkaskaden, deren Auslastung etc. bereit. Die JAP-Software kann mit Hilfe der beim InfoService vorliegenden Daten dem Nutzer eine Vorstellung über den momentanen „Grad seiner Anonymität“ vermitteln. Die gesamte Grobarchitektur lässt sich Abbildung 10 entnehmen.

[472] http://www.anon-online.de/ (letzter Zugriff im Oktober 2007).

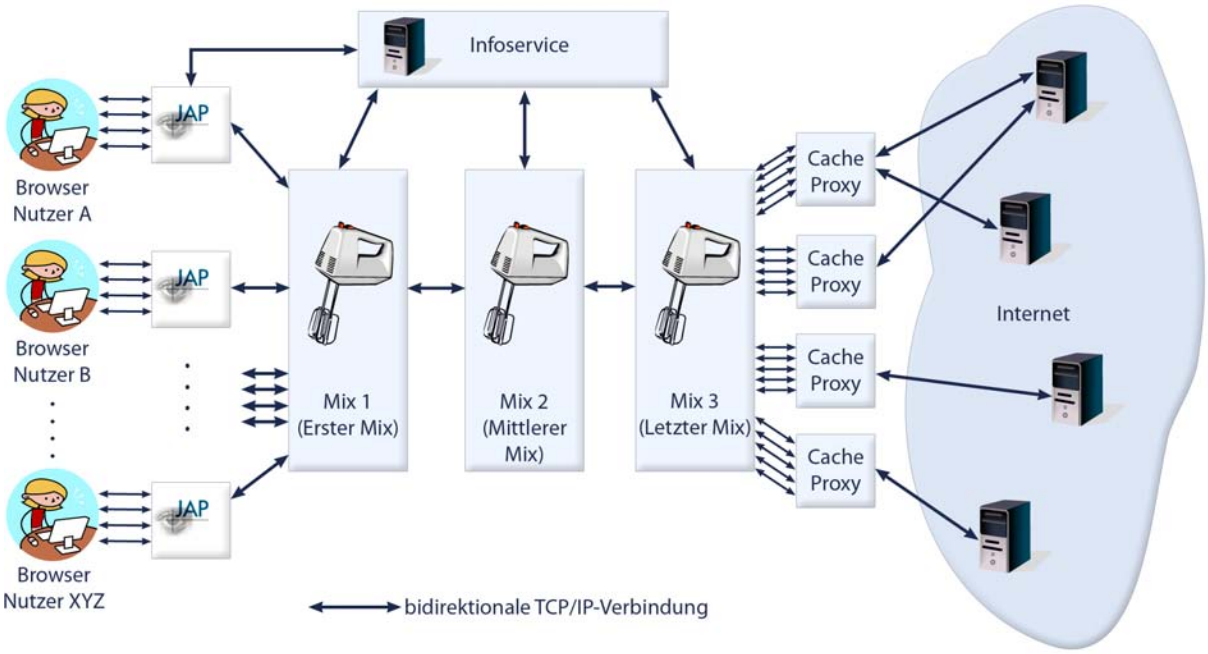


Abbildung 10: Grobarchitektur von AN.ON

4.5.1.2.2 Beispiel „Tor“

Der Anonymisierungsdienst Tor ist eine Weiterentwicklung des Onion-Router-Projekts [Goldschlag/Reed/Syverson 1996], das wiederum auf den Chaumschen Mixen basiert. Entwicklung und Betrieb von Tor werden durch die Electronic Frontier Foundation (EFF) und das U.S. Naval Research Laboratory unterstützt.

Tor verwendet genauso wie AN.ON den Mechanismus der symmetrisch verschlüsselten Kanäle. Während jedoch bei AN.ON auf Grund der Kaskaden die Reihenfolge der Mixe nicht durch den Nutzer beeinflussbar ist, verwendet Tor so genannte freie Mixketten, d.h., der Nutzer kann für jeden Kanal bestimmen, welche Mixe in welcher Reihenfolge verwendet werden sollen.

Ein grundlegender Unterschied zwischen Tor und AN.ON ergibt sich auch aus dem Verfahren zur Etablierung des symmetrischen Kanalschlüssels. Tor verwendet dazu das Diffie-Hellman-Schlüsselaustauschprotokoll, um die notwendigen Geheimnisse für die Kanalverschlüsselung zu generieren.

Ein weiterer Unterschied beim Kanalaufbau besteht darin, dass bei AN.ON mit einem einzigen Verbindungsaufbaupaket, das durch alle Mixe der Kaskade geschickt wird, mit allen Mixen jeweils ein symmetrischer Kanalschlüssel etabliert wird. Bei Tor erfolgt der Kanalaufbau „teleskopartig“, d.h., es wird zunächst mit dem ersten Mix der Kette ein Kanal aufgebaut. Über diesen wird dann ein Verbindungsaufbaupaket zum zweiten Mix der Kette gesendet. Ist auch dieser Kanal aufgebaut, so wird er benutzt, um ein Verbindungsaufbaupaket zum dritten Mix zu senden usw.

4.5.1.3 DC-Netz-Konzept

In [Chaum 1985a], [Chaum 1985] und [Chaum 1988] gibt David Chaum eine von ihm DC-Netz[473] genannte Möglichkeit zum anonymen Senden an. Diese Möglichkeit zum anonymen Senden (und unbeobachtbaren Empfangen) wurde in [Pfitzmann 1985, S. 40-41] zur im Folgenden beschriebenen Möglichkeit verallgemeinert:

[473] „DC-network“ als Abkürzung für „Dining Cryptographers network“; der Name ist passend zu seinem Einführungsbeispiel gewählt. Zusätzlich sei erwähnt, dass er sich aus David Chaums Initialen ergibt.

Bekanntlich bildet jedes endliche Alphabet bezüglich einer ab 0 beginnenden Nummerierung seiner Zeichen und der Addition (modulo der Alphabetgröße) bezüglich dieser Nummerierung eine abelsche Gruppe. Wie üblich werde unter der Subtraktion (eines Zeichens) die Addition seines inversen Gruppenelements verstanden. Das verallgemeinerte überlagernde Senden geschieht dann folgendermaßen:

Teilnehmerstationen erzeugen für jedes zu sendende Nutzzeichen ein oder mehrere Schlüsselzeichen zufällig und gemäß einer Gleichverteilung. Jedes dieser Schlüsselzeichen teilen sie genau einer anderen Teilnehmerstation mittels eines (noch zu diskutierenden) Konzelation garantierenden Kanals mit. Wer mit wem solch einen Konzelation garantierenden Kanal unterhält, muss nicht geheimgehalten werden, sondern sollte sogar, um Angriffen gegen die Diensterbringung leichter begegnen zu können, öffentlich bekannt sein. Jede Teilnehmerstation addiert (modulo Alphabetgröße) lokal alle von ihr erzeugten Schlüsselzeichen, subtrahiert (modulo Alphabetgröße) davon lokal alle ihr mitgeteilten Schlüsselzeichen und addiert (modulo Alphabetgröße), sofern sie ein Nutzzeichen senden will, lokal ihr Nutzzeichen. Dieses Addieren (bzw. Subtrahieren) modulo der Alphabetgröße des verwendeten Alphabets wird Überlagern genannt. Jede Teilnehmerstation sendet das Ergebnis ihrer lokalen Überlagerung (daher der den Mechanismus betonende Name überlagerndes Senden). Alle gesendeten Zeichen werden global überlagert (modulo Alphabetgröße addiert) und das entstehende Summenzeichen an alle Teilnehmerstationen verteilt.

Da jedes Schlüsselzeichen genau einmal addiert und subtrahiert wurde, sich nach der globalen Überlagerung also alle Schlüsselzeichen gegenseitig wegheben, ist das Summenzeichen die Summe (modulo Alphabetgröße) aller gesendeten Nutzzeichen. Wollte keine Teilnehmerstation senden, ist das Summenzeichen das 0 entsprechende Zeichen; wollte genau eine Teilnehmerstation senden, ist das Summenzeichen gleich dem gesendeten Nutzzeichen.

Wählt man als Alphabet die Binärzeichen 0 und 1, so erhält man den für praktische Zwecke wichtigen, von David Chaum angegebenen Spezialfall des binären überlagernden Sendens, bei dem zwischen Addition und Subtraktion von Zeichen nicht zu unterschieden werden braucht.

Natürlich können (digitale) Überlagerungs-Kollisionen auftreten, falls mehrere Teilnehmerstationen gleichzeitig senden wollen: Alle Stationen erhalten die (wohldefinierte) Summe des gleichzeitig Gesendeten. Kollisionen sind ein übliches Problem bei Verteil-Kanälen mit Mehrfachzugriff, zu dessen Lösung es eine große Zahl von Zugriffsverfahren gibt. Alle publizierten Zugriffsverfahren sind auf (analoge) Übertragungs-Kollisionen, z.B. in Bussystemen (wie bei Ethernet), Funk- und Satellitennetzen, ausgelegt, bei denen es kein wohldefiniertes „Kollisionsergebnis“ gibt. Die „Arbeitsbedingungen“ der Zugriffsverfahren sind beim überlagernden Senden in dieser Hinsicht also wesentlich besser als bei üblichen Verteil-Kanälen. Allerdings darf man natürlich nur solche Zugriffsverfahren verwenden, die die Anonymität des Senders und – wenn möglich – auch die Unverkettbarkeit von Sendeereignissen erhalten. Daneben sollten sie bei zu erwartender Verkehrsverteilung den zur Verfügung stehenden Kanal günstig nutzen. Beispiele anonymer und nichtverkettender Zugriffsverfahren sind das einfache, aber nicht sehr effiziente Verfahren „Slotted ALOHA“ und eine für Kanäle mit großer Verzögerungszeit entworfene, effiziente Reservierungstechnik ([Tanenbaum 1981, S. 272], [Chaum 1985a]).

Vereinbart man, dass ein Teilnehmer einen Übertragungsrahmen, in dem er ohne Kollision gesendet hat, weiter benutzen darf und andere Teilnehmer in diesem Rahmen erst wieder senden dürfen, wenn er einmal nicht benutzt wurde, so kann man durch die Verwendung mehrerer Übertragungsrahmen („slots“) sehr effizient Kanäle schalten (siehe [Höckel 1985], [Höckel/Pfitzmann 1985]). Natürlich ist alles, was über solch einen Kanal gesendet wird, verkettbar – andererseits werden Kanäle typischerweise für solche Dienste verwendet, in deren Natur dies liegt.

4.5.2 Techniken zur Erreichung von Authentizität und Zurechenbarkeit

4.5.2.1 Allgemeines zu digitalen Signaturen

Mit einer digitalen Signatur unter einer Nachricht oder Aktion wird nicht nur die Integrität der Nachricht oder Aktion, sondern auch die Zurechenbarkeit des Signierers sichergestellt. In einem entsprechenden digitalen Signatursystem muss hierzu derjenige, der Nachrichten oder Aktionen signieren möchte, ein Schlüsselpaar bestehend aus privatem und öffentlichem Schlüssel generieren. Ersterer ist nur ihm bekannt und nur mit diesem können (unter Annahme bestimmter kryptographischer Annahmen) Signaturen unter Nachrichten oder Aktionen erzeugt worden sein. Den öffentlichen Schlüssel verteilt er vorab auf vertrauenswürdige Weise an mögliche Interakteure, die seine digitalen Nachrichten erhalten oder durch seine Aktionen kontaktiert werden sollen. Jeder dieser Interakteure wird damit in die Lage versetzt, die Korrektheit der Signaturen unter den Nachrichten oder Aktionen zu überprüfen. In Abbildung 11 ist ein digitales Signatursystem schematisch dargestellt.

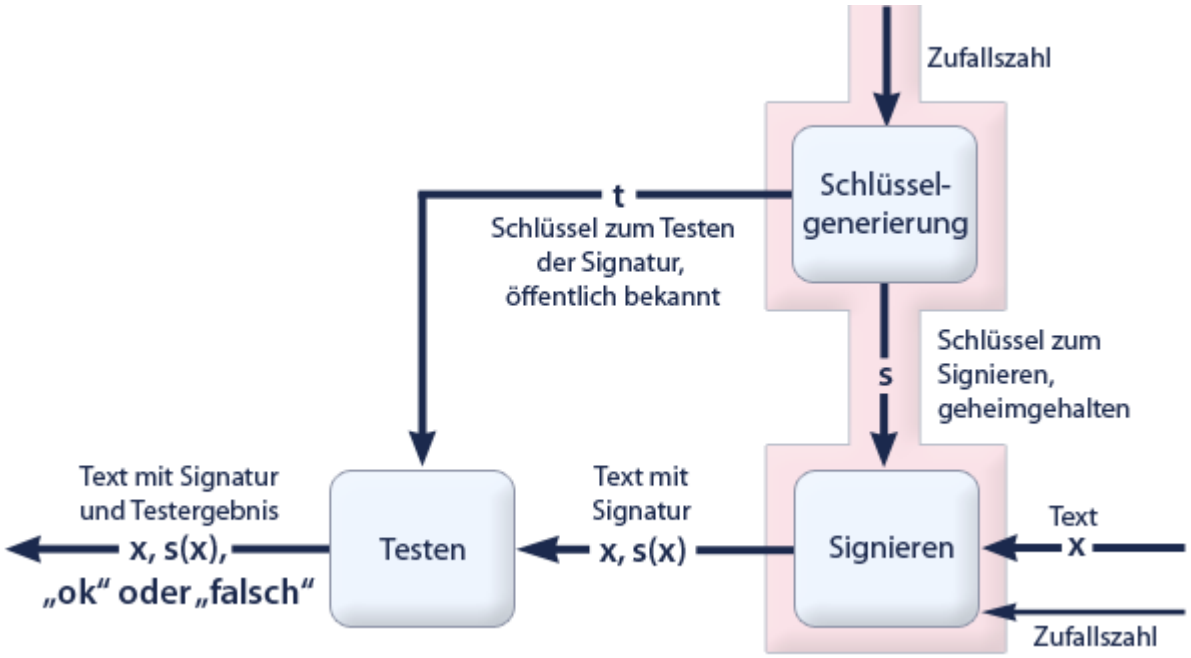


Abbildung 11: Schema eines digitalen Signatursystems

Für Signatursysteme existieren etablierte kryptographische Mechanismen wie RSA [Rivest/Shamir/Adleman 1978], DSS [FIPS 1994] oder Schnorr-Signaturen [Schnorr 1991].

4.5.2.2 Nicht herumzeigbare Signaturen

Übliche digitale Signaturen können leicht perfekt kopiert und deshalb unbeschränkt herumgezeigt werden. Abhilfe schafft hier die Idee, das Testen einer Signatur nicht als vom Empfänger autonom durchführbaren deterministischen Algorithmus vorzusehen, sondern als ein interaktives Protokoll, zu dem man denjenigen braucht, der die Signatur angeblich geleistet hat. So erfährt er, wenn ein Dritter seine Signatur erhalten soll. („Erhalten" bedeutet hier nicht nur, die entsprechende Bitkette zu erfahren, sondern auch Gewissheit zu erlangen, dass es sich um eine gültige Signatur handelt.) Wichtig bei der Gestaltung des Protokolls ist, dass der Unterzeichner eine echte Signatur nicht ableugnen kann (deshalb die englische Bezeichnung von David Chaum: „undeniable"): Betrügt er

beim Protokoll, so wird er mit einer Wahrscheinlichkeit exponentiell nahe bei 1 erwischt. Macht er beim Protokoll nicht mit, obwohl er dazu verpflichtet ist, gilt dies als Beweis für die Echtheit der Signatur. Abbildung 12 zeigt ein solches Signatursystem.

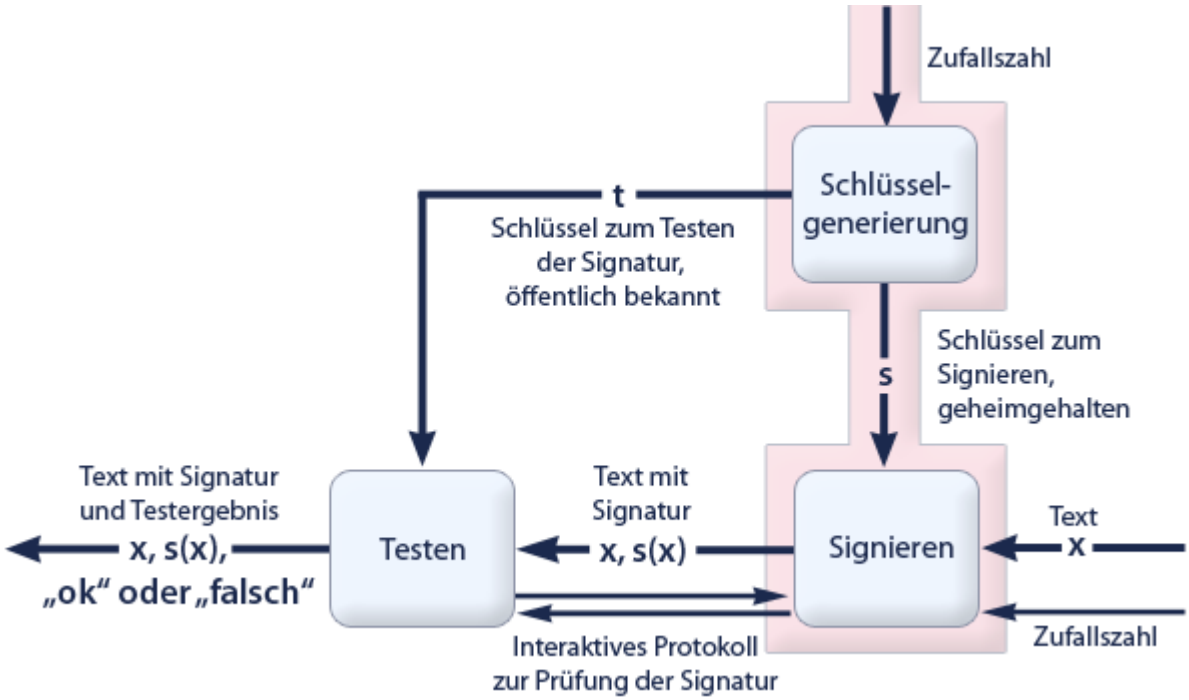


Abbildung 12: Digitales Signatursystem für nicht herumzeigbare Signaturen

4.5.3 Authentizität und Vertraulichkeit der Kommunikationsumstände

In diesem Abschnitt wird zunächst das grundlegende Konzept des Pseudonyms vorgestellt. Darauf aufbauend werden Techniken beschrieben, die Authentizität und Zurechenbarkeit von unter Pseudonym ausgetauschten Daten für verschiedene Zwecke ermöglichen.

4.5.3.1 Konzept des Pseudonyms allgemein

Die Stärke der Anonymität eines Nutzers in einer Interaktion mit anderen wird nicht nur durch die Kennzeichen bestimmt, die der Partner automatisch über den Benutzer erfährt, etwa Art und Uhrzeit des abgewickelten Geschäfts, sondern vor allem durch eigens gewählte Kennzeichen wie Kennnummern oder Testschlüssel für digitale Signaturen, so genannte Pseudonyme.

Eine aus praktischer Sicht zweckmäßige grobe Einteilung von Pseudonymen nach der Stärke der durch sie realisierten Anonymität ist in Abbildung 13 dargestellt.

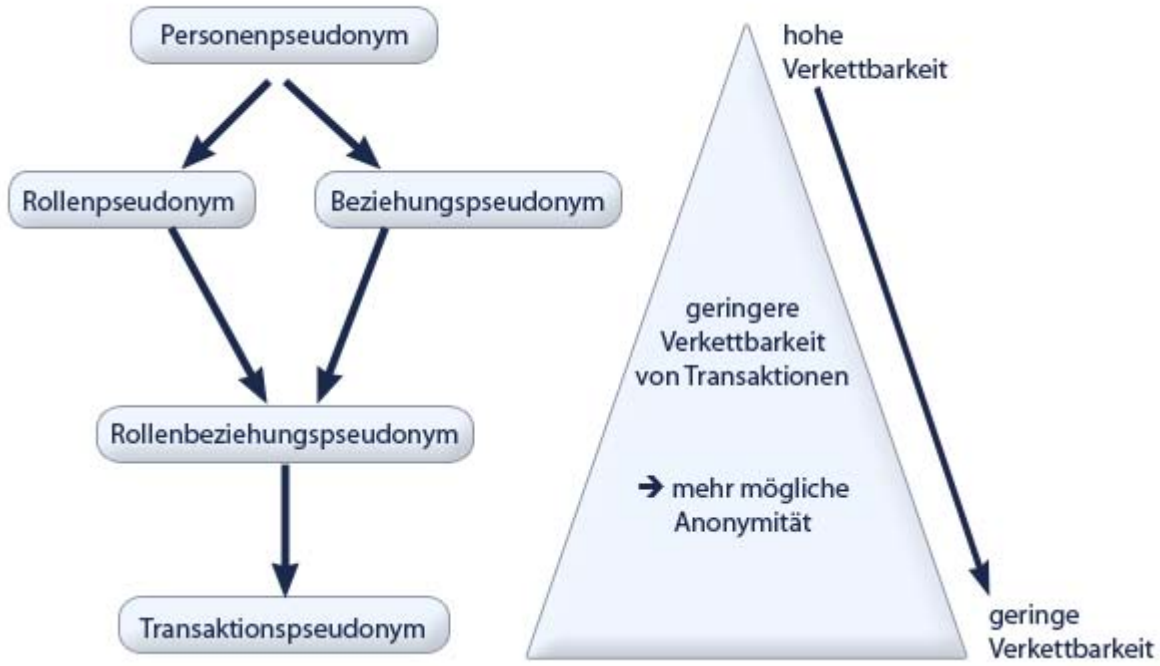


Abbildung 13: Pseudonymtypen nach ihren Verkettbarkeitseigenschaften

Ein Pseudonym wird als Personenpseudonym bezeichnet, wenn sein Inhaber es für viele verschiedene Geschäftsbeziehungen über lange Zeit hinweg verwendet, es somit einen Namensersatz darstellt. Bei Verwendung von Personenpseudonymen sammelt sich bei einem Beobachter laufend personenbezogene Information an, so dass nach einer gewissen Zeit der Inhaber eines Personenpseudonyms identifiziert werden kann. Jedes Personenpseudonym ist ein potenzielles Personenkennzeichen.

Diesen Nachteil vermeiden Rollenpseudonyme, die im Gegensatz zu Personenpseudonymen nicht der Person, sondern nur ihrer momentan ausgeübten Rolle zugeordnet sind.

Neben der Unterscheidung nach Rollen können Pseudonyme auch unterschiedlichen Kommunikationsbeziehungen zugeordnet werden. Beziehungspseudonyme werden hierbei jeweils für Kommunikationsbeziehungen zu genau einem Kommunikationspartner verwendet.

Ein Rollenbeziehungspseudonym wird für die Kommunikation mit genau einem Kommunikationspartner in genau einer Rolle verwendet.

Transaktionspseudonyme hingegen werden nur für eine Transaktion verwendet, z.B. Kennwörter bei anonym aufgegebenen Chiffreanzeigen. Bei Verwendung von Rollenpseudonymen können verschiedene Parteien über den Pseudonymträger gesammelte Information zumindest nicht einfach über die Gleichheit von Pseudonymen, sondern allenfalls über Korrelation von Zeiten, Geldbeträgen etc. verketten. Aber trotzdem besteht bei Geschäftsbeziehungspseudonymen das Risiko, dass bei intensiv genutzten Beziehungen der Partner genügend pseudonymbezogene Information zur Deanonymisierung erhält. Aus der Sicht der Vertraulichkeit sollten daher, wenn immer möglich, Transaktionspseudonyme verwendet werden.

Kommunikation zwischen solchermaßen voreinander anonymen Partnern ist über ein Verkehrsdaten schützendes Kommunikationsnetz ohne weiteres möglich, denn es gestattet, Nachrichten ohne Absenderangabe zu senden und unter beliebigen Pseudonymen zu empfangen, die nicht (wie sonst Adressen) den physischen Ort des Benutzers oder gar ihn selbst bezeichnen. Ebenso wenig wird die Verwendung eines kryptographischen Systems erschwert, da die Schlüssel eines asymmetrischen kryptographischen Systems, das entweder selbst zum Verschlüsseln oder zum Schlüsselaustausch

für ein symmetrisches System verwendet wird, statt identifizierbaren Benutzern auch Pseudonymen zugeordnet sein können.

4.5.3.2 Eigenschaften digitaler Pseudonyme

Zunächst ist ein digitales Pseudonym ein in IT-Systemen verwendbares Kennzeichen (z.B. eine natürliche Zahl). Um ein solches Pseudonym im Hinblick auf Verkettbarkeit einsetzen zu können, muss es in einem definierten Bereich eindeutig sein. Ein Beispiel hierfür ist ein so genannter „Universally Unique Identifier“ (UUID), d.h. ein z.T. zufällig generiertes Kennzeichen, das so erzeugt wird, dass es mit sehr hoher Wahrscheinlichkeit global eindeutig ist. Während ein solcher UUID unabhängig von dem damit bezeichneten Objekt ist, kann auch ein eindeutiges Kennzeichen auch aus der (eindeutigen) Beschreibung des zu bezeichnenden Objektes mit Hilfe von kryptographischen Operationen, z.B. einer kollisionsresistenten Hashfunktion, gewonnen werden. Ein solches Verfahren sorgt dafür, dass das Pseudonym effizient aus der Beschreibung des Objektes erzeugt werden kann, aber die Umkehrung mit verfügbaren technischen Mitteln nicht möglich ist.

Eine weitere wichtige Eigenschaft von digitalen Pseudonymen ist die Möglichkeit, beliebige Daten beweisbar an diese Pseudonyme zu binden. Dies kann zum Beispiel geschehen, indem ein digitales Pseudonym gleichzeitig der öffentliche Schlüssel eines digitalen Signatursystems ist, bzw. gemeinsam mit einem digitalen Signatursystem verwendet wird. Diese Eigenschaft ermöglicht es, verschiedene Daten nachweisbar miteinander zu verketten. Dies ermöglicht insbesondere eine Verwendung von Pseudonymen für eine sichere Authentikation, da Autorisierungstoken beweisbar an ein Pseudonym gebunden werden können.

4.5.3.3 Blinde Signaturen

In Anwendungen, wo ein Signierer lediglich die Integrität von einem digitalen Dokument sichern soll, nicht aber den Inhalt dessen, was er signiert, kennen muss bzw. soll, findet ein blindes Signatursystem Einsatz.

Wie bei traditionellen Signatursystemen wird vom Signierer ein Schlüsselpaar aus öffentlichem und privatem Schlüssel generiert und der öffentliche Schlüssel an alle verteilt, die später seine Signaturen testen möchten. Im Gegensatz zu traditionellen Signatursystemen wird das zu signierende Dokument dann jedoch nicht vom Signierer, sondern von demjenigen, der sich dessen Signatur auf dieses Dokument wünscht, erstellt und geblendet (üblicherweise mit Verschlüsselung) und an den Signierer zum Zwecke des Signierens gesendet. Nach Erhalt des signierten Dokuments weiß nur der Ersteller des Dokuments, wie er das Dokument wieder entblenden und die Signatur auf dem geblendeten Dokument in eine auf dem entblendeten Dokument umrechnen kann. Jeder, der den öffentlichen Schlüssel des Signierers kennt, kann die Integrität von dessen Signatur unter dem entblendeten Dokument testen. Gleichzeitig wird Unverkettbarkeit von ent- und geblendetem Dokument und Unverkettbarkeit der zugehörigen Signaturen erreicht.

Blinde Signatursysteme können unter Verwendung vieler traditioneller Signatursysteme implementiert werden, z.B. RSA [Rivest/Shamir/Adleman 1978].

4.5.3.4 Credential-Systeme

In einem Credential- oder Beglaubigungssystem können Entitäten von anderen Entitäten Credentials bzw. Beglaubigungen über Eigenschaften oder Rechte erhalten und deren Besitz gegenüber dieser und ggf. weiteren Entitäten nachweisen. Diese Vorzeigbarkeit wird durch die Integrität der Beglaubigung bzgl. der ausstellenden Entität gewahrt.

Wenn Credentials an Pseudonyme vergeben werden, werden sie als pseudonyme Credentials bezeichnet.

Mit *pseudonymen umrechenbaren Credentials* (engl.: *„pseudonymous convertible credentials“*) werden Nutzer in die Lage versetzt, die auf eines ihrer Pseudonyme ausgestellte Beglaubigung auf ein anderes ihrer Pseudonyme umzurechnen. Trotzdem bleiben die Integrität der Beglaubigung bzgl.

der ausstellenden Entität und damit die Möglichkeit der Vorzeigbarkeit erhalten. Gleichzeitig wird aber Unverkettbarkeit von Beglaubigung und umgerechneter Beglaubigung hergestellt und damit eine bestehende Unverkettbarkeit der zugehörigen Pseudonyme erhalten. Diese Idee wurde in [Chaum 1985] vorgestellt. Es gibt zahlreiche Implementierungsmöglichkeiten: In [Camenisch/Lysyanskaya 2001] wurde ein auf der starken RSA-Annahme und der Diffie-Hellman-Entscheidungs-Annahme (engl.: „decisional Diffie-Hellman assumption“) basierendes System vorgestellt. Dort wird das System als anonymes Beglaubigungssystem bezeichnet. Demgegenüber priorisieren die Verfasser den Begriff des *pseudonymen Beglaubigungssystems*, da das System nicht direkt Anonymität erreicht, sondern nur Pseudonymität durch die Verwendung von Pseudonymen und deren Unverkettbarkeit unterstützt. Dies kann zu einem anonymen System führen, tut es aber nicht zwangsläufig, wenn zu Entitäten verkettbare Pseudonyme genutzt werden.

4.5.3.5 Gruppensignaturen

Wenn die Integrität einer Nachricht oder Aktion mit einer *Gruppensignatur* [Chaum/Heyst 1991] gesichert wird, dann gilt in Abweichung zu traditionellen Signatursystemen für Kommunikationspartner oder Interakteure außerhalb dieser Gruppe nicht die Integrität und Zurechenbarkeit bzgl. des konkreten Absenders bzw. Akteurs, sondern bzgl. der Gruppe, zu der der Absender bzw. Akteur gehört. D.h., derjenige ist innerhalb dieser Gruppe für Außenstehende anonym, und seine Signaturen sind unverkettbar. Die Mitglieder der Gruppe bzw. ihr Gruppenmanager können hingegen unter bestimmten Umständen einer Gruppensignatur deren Urheber zuordnen. Für Prüfung dieser Signaturen gibt es für Außenstehende wie bei traditionellen Signatursystemen einen öffentlichen Schlüssel. Für die Verteilung der zum Signieren nötigen privaten Schlüssel innerhalb der Gruppe sind verschiedene Algorithmen nötig, insbesondere auch solche, die die Aufnahme neuer Mitglieder und den Ausschluss bestehender Mitglieder ermöglichen.

4.5.3.6 Zero-Knowledge-Verfahren

Bei *Zero-Knowledge-Verfahren* handelt es sich um spezielle interaktive Beweissysteme, die es einem Teilnehmer – dem Beweiser – ermöglichen, einen anderen Teilnehmer – den Verifizierer – zu überzeugen, über ein bestimmtes geheimes Wissen zu verfügen, ohne dieses Wissen preisgeben zu müssen. Das Konzept des Zero-Knowledge-Verfahrens wurde erstmals 1985 von Goldwasser, Micali und Rackhoff vorgestellt [Goldwasser/Micali/Rackoff 1985].

Aus der Sicht des Verifizierers sind die Antworten des Beweisers in einem Zero-Knowledge-Verfahren damit äquivalent zu einer 1-Bit-Antwort eines vertrauenswürdigen Orakels [Feige 1990]. Solche Beweissysteme eignen sich daher insbesondere für Identifikations- und Authentifikationsverfahren. Dabei führt ein sich identifizierender Teilnehmer einen Beweis zu einer bestimmten (mathematischen) Behauptung durch, der ihm nur gelingen kann, wenn er über das ihn identifizierende individuelle Geheimnis verfügt. Die verifizierende Instanz kann dadurch von den Identitäten der jeweiligen Teilnehmer überzeugt werden, ohne etwas über ihre Geheimnisse zu erfahren. Dies ist ein enormer Vorteil gegenüber üblichen Beweisverfahren, wie sie z.B. zur Authentifikation an Bankautomaten eingesetzt werden, denn dabei ist ein Nachweis von Wissen nur durch das Präsentieren des zugehörigen Geheimnisses möglich. Bisher muss ein Teilnehmer zur Authentifikation an Bankautomaten seine persönliche Geheimzahl (PIN) eingeben, so dass jeder, der diese Eingabe beobachtet, das Geheimnis des Teilnehmers erfährt. Zudem muss die PIN auch dem Banksystem bekannt sein, wo sie als Vergleichswert benötigt wird. Mit Hilfe von Zero-Knowledge-Verfahren können hingegen Authentifikationssysteme erstellt werden, in denen die PIN nie den „sicheren“ Chip verlassen muss und damit auch niemandem, außer dem Teilnehmer selbst, bekannt ist.

Die oben vorgestellten pseudonymen Beglaubigungssysteme (engl.: „pseudonymous convertible credentials“) basieren im Wesentlichen auf Zero-Knowledge-Verfahren.

4.6 Nutzergesteuertes Identitätsmanagement

Identitätsmanagement bedeutet das Verwalten von (Teil-)Identitäten und/oder von Identitätsdaten. In der Regel handelt es sich um das Managen von Teilidentitäten einer (natürlichen) Person, d.h. das Verwalten von Identitätsattributen einschließlich der Weiterentwicklung und Auswahl von Teilidentität und Pseudonym, die dann in einem spezifischen Kontext oder einer Rolle (wieder-)verwendet werden.

Identitätsmanagementsysteme, d.h. Kombinationen aus Software, Hardware und Prozessen, bieten ein technisch gestütztes Identitätsmanagement. Diese Systeme lassen sich unter den Gesichtspunkten des Durchführenden des Managements, der Ziele des Managements und der hierfür eingesetzten Methoden in drei grundsätzliche Typen gliedern [Bauer/Meints/Hansen 2005]:

- *Typ 1:* Systeme für Account-Management;
- *Typ 2:* Systeme für Profiling (vgl. Abschnitt 3.3.3);
- *Typ 3:* Systeme für nutzergesteuertes Identitätsmanagement.

Kombinationen dieser Typen sind möglich. Für alle Identitätsmanagementsystemtypen sind Realisierungen denkbar, die verkettungsarm sind, d.h. den Grad an Verkettbarkeit nicht oder nicht wesentlich erhöhen. In diesem Fällen spricht man von *„Privatheit förderndem Identitätsmanagement“* (engl.: *„privacy-enhancing identity management“*, vgl. [Pfitzmann/Hansen 2007]).

Ziel des *nutzergesteuerten Identitätsmanagements* (engl.: *„user-controlled identity management“*) ist es, den Nutzern zu ermöglichen, selbst die Kontrolle über ihre Privatsphäre zu übernehmen. Jeder Nutzer soll selbst einschätzen und bestimmen können, welche seiner Kommunikationspartner was über ihn wissen. Genau dies fordert das Recht auf informationelle Selbstbestimmung, wie es 1983 im Bundesverfassungsgerichtsurteil zur Volkszählung formuliert wurde.

Dabei spielt Verkettbarkeit eine ganz zentrale Rolle: Nutzergesteuertes und zugleich Privatheit förderndes Identitätsmanagement soll Verkettungen der digitalen Nutzeridentitäten nur ermöglichen, wenn dieser es möchte. Ansonsten sollte Unverkettbarkeit soweit wie möglich realisiert werden.

Wichtige Funktionalitäten des nutzergesteuerten Identitätsmanagement sind (vgl. [IMS Study 2003], [Hansen/Borcea-Pfitzmann/Pfitzmann 2005] sowie [Leenes/Schallaböck/Hansen 2007]):

- *Verwaltung der eigenen digitalen Identitäten:*
  Art und Umfang der Daten, die ein Nutzer herauszugeben bereit ist, hängen sowohl von den jeweiligen Kommunikationspartnern ab als auch von seiner Rolle, in der er Informationen über sich kommuniziert. Nutzergesteuerte Identitätsmanagementsysteme ermöglichen eine kontextabhängige Herausgabe von Identitätsdaten. Um dem Nutzer veranschaulichen zu können, was er an die verschiedenen Kommunikations- und Transaktionspartner herausgegeben hat, werden die Preisgaben von Daten mitgeloggt. Im Prototyp des Projekts „PRIME – Privacy and Identity Management for Europe“[474] heißt diese Funktion „Data Track“.
- *Datensparsamkeit:*
  Vielfach kann bei der Inanspruchnahme von Diensten auf Daten, die den Nutzer identifizieren, verzichtet werden. Dies unterstützt das Identitätsmanagementsystem durch die Bereitstellung von Pseudonymen oder sogar anonymen Nutzungsmöglichkeiten ganz ohne Offenbarung persönlicher Daten. Damit soll die Verkettbarkeit der Nutzerdaten durch Unberechtigte verhindert oder zumindest eingeschränkt werden. Für eine möglichst weitgehende Einschränkung der Verkettungsmöglichkeit sollen Pseudonyme nicht kontextübergreifend eingesetzt werden. Stets kann der Nutzer sich aber dafür entscheiden, eine Verkettung – ggf. auch kontextübergreifend – explizit zuzulassen. Auch Credentials (vgl. Abschnitt 4.5.3.4) als Mittel, um Anonymität und Zurechenbarkeit zu kombinieren, ohne dass jedes Vorzeigen eines Credentials verkettbar wird, kommen beim nutzergesteuerten Identitätsmanagement zum Einsatz.
- *Aushandlung über Datenschutzbedingungen:*
  Ist keine anonyme Nutzung der Dienste möglich, können digitale Policies die Vorstellungen

[474] https://www.prime-project.eu/ (letzter Zugriff im Oktober 2007).

des Nutzers, wann er wem welche Daten unter welchen Bedingungen offenbart, zum Ausdruck bringen und dem Datenverarbeiter mitgeteilt werden. Diese lässt sich mit den Angaben zur Datenverarbeitung aus der Privacy Policy der Gegenseite abgleichen. Stimmen die Vorstellungen nicht überein, wird hier gegebenenfalls eine Aushandlung erforderlich. Für eine spätere Nachvollziehbarkeit speichert das Identitätsmanagementsystem auf Nutzerseite mit, welche Datenschutzbedingungen ausgehandelt wurden.

Auch wenn heutige Prototypen für nutzergesteuertes Identitätsmanagement hauptsächlich den Internetbereich adressieren, sind übergreifende Ansätze denkbar, die alle Phasen im Lebenszyklus digitaler Identitäten (vgl. [Hansen/Meints 2006]) umfassen.

4.7 Reputationssysteme

4.7.1 Allgemeines

Wie bereits in Abschnitt 2.3.4.2 ausgeführt, haben Nutzer neben den Anforderungen an IT-Systeme vorrangig auch die Erwartung an das Verhalten der Interakteure, dass diese versuchen, die Anforderungen auch auf semantischer Ebene zu garantieren. Die Erfüllung der Erwartungen ist bei der Interaktion mit Unbekannten (wie zumeist im Internet) in der Regel wesentlich ungewisser als bei der Interaktion mit bereits bekannten Menschen. Das Risiko des Einzelnen bei einer Interaktion ist insbesondere beim Online-Handel monetär zu messen.

In der realen Welt wird versucht, Erwartungen von Unbekannten aneinander in Vereinbarungen festzuhalten, die durch Verträge gesichert werden: die handschriftliche Unterschrift soll die juristische Zurechenbarkeit zu einer Aussage sichern. Eine entsprechende Zurechenbarkeit zu den innerhalb einer Internet-Community erlaubten Handlungen wünschen sich deren Mitglieder ebenso. Auch jede digitale Information kann durch Hinzufügen einer digitalen Signatur (und ggf. eines Zeitstempels) integer (und speziell authentisch bzgl. des Urhebers) gemacht werden und so rechtlich der handschriftlichen Unterschrift gleichgestellt werden. Dadurch können jedoch – ebenso wie in der realen Welt – den Mitgliedern nur Beweise für das Fehlverhalten eines anderen geliefert werden. Jede Art von Disput muss außerhalb des IT-Systems im juristischen Prozess gelöst werden. Die genaue juristische Zurechenbarkeit von digitalen Handlungen hängt davon ab, inwieweit die sie sichernden technischen Maßnahmen im nationalen und internationalen Recht als rechtlich bindend angesehen werden. Der juristische Prozess ist zudem teuer und aufwändig für denjenigen, der die Zurechenbarkeit durchsetzen möchte, und sollte aus seiner Sicht vermieden werden. Umgekehrt sind mögliche rechtliche Konsequenzen für denjenigen, der sich entgegen seiner vorher zugesicherten Aussage verhalten möchte, hoffentlich abschreckend genug, dies doch nicht zu tun.

Jede menschliche Interaktion setzt deshalb vorab ex- oder implizites Vertrauen (engl.: „trust“) in den Interakteur voraus, dass es gar nicht erst soweit kommt, dass juristische Maßnahmen ergriffen werden müssen. Idealerweise basiert das Vertrauen auf bisherigen Erfahrungen mit dem Interakteur, was in vielen Internet-Communities jedoch insbesondere für neue Mitglieder meist nicht gegeben ist.

Wenn einem Nutzer eigene Erfahrungen in der Interaktion mit einem anderen fehlen, können ihm gegebenenfalls Erfahrungen anderer helfen. Während dies in der realen Welt meist durch Mundpropaganda geschieht, kann dies in der digitalen Welt technisch effizient mit Reputationssystemen realisiert werden. Reputationssysteme sammeln die Erfahrungen, die Nutzer in der Interaktion mit anderen sammeln. Nutzer bauen somit eine Reputation innerhalb der Internet-Community auf. Vom lateinischen Wortstamm her bedeutet *Reputation* wörtlich „Erwägung“ bzw. „Betrachtung“. Diese Betrachtung eines Nutzers durch Interakteure liefert anderen Nutzern vor der Interaktion mit Unbekannten einen Anhaltspunkt über deren bisheriges Verhalten und hilft hoffentlich, zukünftige Erfahrungen abzuschätzen. Diese Hoffnung gründet sich darauf, dass Interakteure meist einen Gewinn aus Interaktionen ziehen und ein Fehlverhalten wiederum in das Reputationssystem einfließen würde und damit ihren Gewinn in zukünftigen Interaktionen mindern könnte.

In der realen Welt kann meist der Wert von Mundpropaganda abhängig vom Kontext abgeschätzt werden; in der digitalen Welt ist dies viel weniger der Fall. Beim Design von Reputationssystemen

sollte deshalb berücksichtigt werden, dass der technisch erfassbare Kontext der Erfahrungen in einer Interaktion bei der Konstruktion der resultierenden Reputation der Interakteure einbezogen werden kann, um Nutzern zu ermöglichen, die Glaubwürdigkeit von Reputation selbst abzuschätzen. Kontextinformationen aus Interaktionen können beispielsweise Zeitpunkt oder Bedeutung der Interaktion für die beiden Interakteure sowie Reputation des wertenden Interakteurs sein.

Reputation von Mitgliedern erlaubt, andere Menschen als geeignete Interakteure auszuwählen, die sich mit hoher Wahrscheinlichkeit an einer Interaktion beteiligen und sich dabei auch korrekt und diskret verhalten. Dabei sind zwei Arten von Reputation zu unterscheiden: *Implizite Reputation* ist an ein bestimmtes Pseudonym gebunden, die eine Person im Laufe der Zeit durch ihr Verhalten in Interaktionen erworben hat. Dies kann ein Mitglied sein, das vielfach innerhalb der Community gute Ratschläge gibt. Wenn ein Nutzer aber gleichzeitig eine akzeptable Anonymität seines Pseudonyms wahren möchte, muss er zwischen der implizit aufgebauten Reputation und der Unverkettbarkeit seiner Handlungen abwägen. Dies mag ein Grund sein, um *explizite Reputation* eines Pseudonyms zu etablieren, die mit Hilfe von Reputationssystemen auf Basis von Erfahrungen anderer Nutzer mit diesem Pseudonym berechnet wird. Explizite Reputation erlaubt einem Nutzer, anonym innerhalb aller Nutzer mit der gleichen Reputation zu sein, solange seine Interaktionsgeschichte nicht öffentlich ist. Wenn Pseudonyme jedoch in vielen Interaktionen und über eine lange Zeit genutzt werden, wird die Anzahl der Pseudonyme mit der gleichen Reputation recht klein werden.

Reputationssysteme als Datenbanken zur Sammlung der bisherigen Erfahrungen von Nutzern und über Nutzer erlauben jedoch nicht nur Mitgliedern einer Internet-Community, sich legitim über andere vor einer geplanten Interaktion zu informieren. Viel mehr üben sie auch einen Reiz auf zahlreiche Datensammler aus, die durch Zugang zu solchen Reputationssystemen umfangreiche Informationen erhalten können, wer wann mit wem in welchem Kontext interagiert hat. Dadurch lassen sich (z.B. marktwirtschaftlich interessante) Profile über Interessen von Nutzern aufbauen.

4.7.2 Reputation in C2C-Communities

Zahlreiche Anbieter offerieren Plattformen, die C2C-Communities oder so genannte „Internet-Marktplätze“ etablieren, deren Mitglieder einander Objekte zum Kauf anbieten und voneinander kaufen dürfen (vgl. auch Abschnitt 3.4.3.3). Wer Mitglied werden möchte, muss sich beim Provider durch Wahl eines in der Community zu verwendenden Pseudonyms und Angabe einiger persönlicher Daten (z.B. Alter, Post- und E-Mail-Adresse) registrieren, die vom Provider ggf. verifiziert werden können. Meist wird zumindest die Gültigkeit der E-Mail-Adresse überprüft.

In [Chui/Zwick 1999] findet sich für den speziellen Fall der Internetauktionen als Internet-Marktplätze ein Überblick über Provider und benutzte Modelle.

Einer der größten Anbieter mit nach eigenen Angaben [eBay 2005] ca. 72 Millionen aktiven Mitgliedern Ende 2005 ist eBay[475]. Das dort verwendete Modell wird in vielen anderen Internet-Marktplätzen ähnlich angewandt und wird im Folgenden weiter als Beispiel verwendet.

Zum weiteren Zugang zur webbasierten Plattform werden dann AAA-Infrastrukturen eingesetzt.

Wenn ein Mitglied der Community ein Objekt verkaufen möchte, muss er ein Angebot aufsetzen, das vom Provider für andere Mitglieder einsehbar veröffentlicht wird. Üblicherweise enthält das Angebot mindestens das Pseudonym des Verkäufers und eine Beschreibung des angebotenen Objekts. Zudem werden typischerweise der Verkaufs-/Auktionszeitraum und Verkaufs-/Mindestpreis angegeben.

eBay macht zum Zwecke der Umsatzsteigerung Gebrauch von Empfehlungssystemen, um Mitgliedern bald endende bzw. zu ihren bisherigen Suchanfragen passende Interaktionen in Form von Verkaufsangeboten zu präsentieren.

Der Austausch von Ware und Gegenwert zwischen einem Verkäufer und Käufer muss fair vonstatten gehen, d.h., Käufer und Verkäufer müssen beide das erhalten, auf das sie sich geeinigt hatten. Geht einer von beiden leer aus, liegt ein Betrug vor (natürlich könnte auch das System versagt haben, was

[475] http://www.ebay.com/ (letzter Zugriff im Oktober 2007).

es aber nicht tun sollte, wenn es sicher ist). Die meisten Verkaufsobjekte sind physische Güter, die entweder direkt zwischen Verkäufer und Käufer oder über eine (hoffentlich vertrauenswürdige) dritte Partei, die korrekten Transfer garantiert, ausgetauscht werden. Viele Provider bieten oder vermitteln diesen Service gegen eine zusätzliche Gebühr.

Einige Anbieter von Marktplätzen, die beschränkt sind auf bestimmte Güter, lassen sich das anzubietende Objekt auch zunächst vom Verkäufer auf Kommission zusenden und erstellen selbst das Angebot für ihren Marktplatz und wickeln den Verkauf ab. Dies ist natürlich nur für leicht beschreibbare und vergleichbare Objekte möglich.

Eine gegen alle Beteiligten (inkl. Auktionator) sichere Implementierung von elektronischen Auktionen, die digitale Signaturen und Zeitstempel nutzt, um Integrität und Zurechenbarkeit von digitalen Handlungen zu sichern, wurde in [Stubblebine/Syverson 1999] vorgestellt. Die benutzten Techniken können einfach auf allgemeine elektronische Marktplätze erweitert werden. Dies setzt aber den Austausch digitaler Ware und digitalen Gelds voraus.

Da auf eBay zumeist physische Güter gehandelt werden, wird dort ein Reputationssystem angewendet, um Mitgliedern ihrer C2C-Community zu helfen, Erfahrungen zwischen Käufern und Verkäufern zu sammeln und hoffentlich zukünftige Erfahrungen abschätzen zu können und insbesondere Probleme zu vermeiden. Ein Beispielprofil findet sich in Abbildung 14.

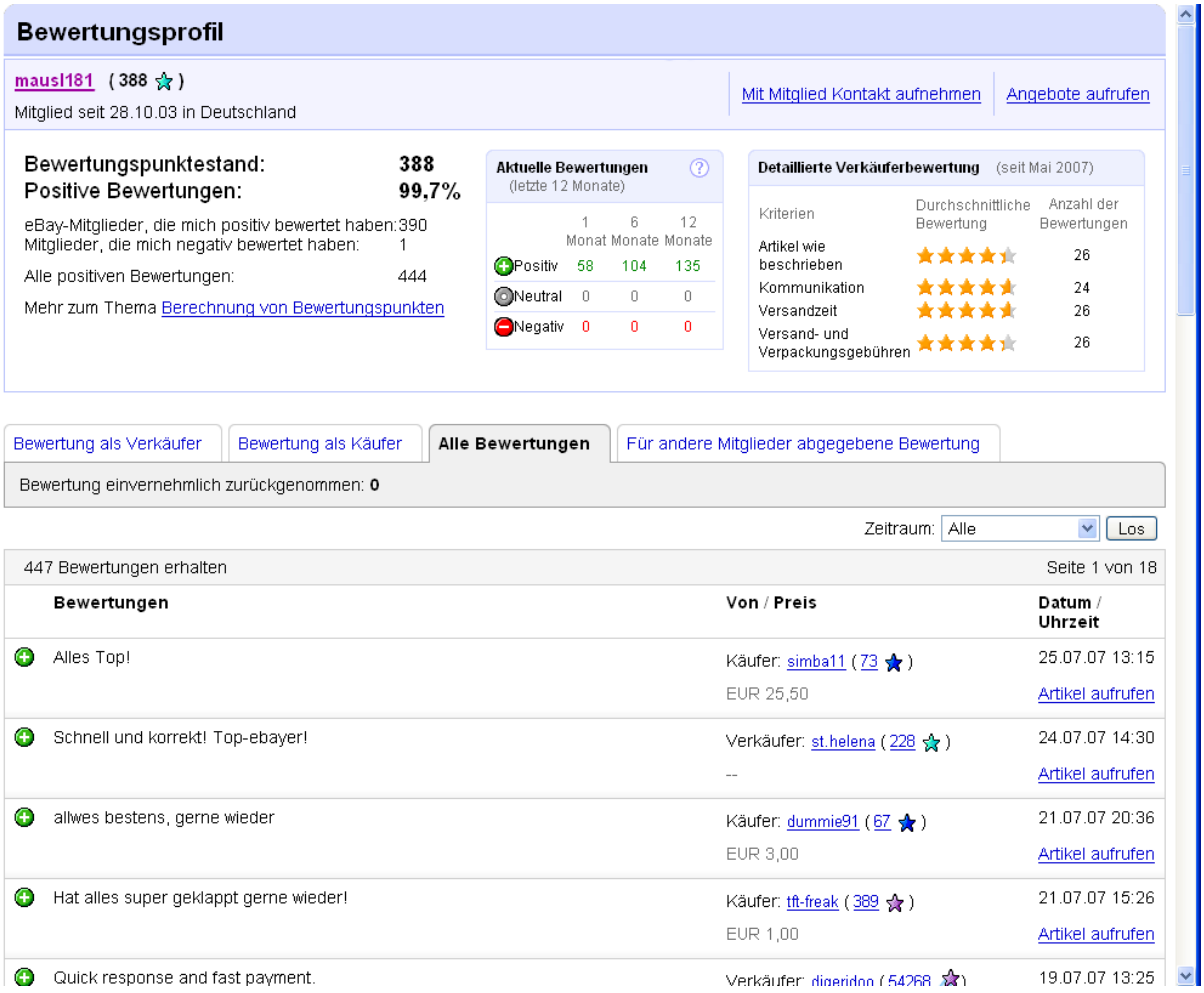


Abbildung 14: Screenshot: Beispielprofil bei eBay

Leider erlauben die derzeit gebräuchlichen Reputationssysteme [Kollock 1999] (an deren Technologie sich in den vergangenen Jahren wenig geändert hat) die Erstellung von Interessens- und Verhaltensprofilen zu Pseudonymen (z.B. Zeit und Häufigkeit der Teilnahme an Internetauktionen, Wertschätzung von und Interesse an bestimmten Gütern). Sobald das Pseudonym zu personenbezogenen Daten einer Person verkettet werden kann, wie es typischerweise für Handelspartner möglich ist, wird auch das Profil zu dieser Person verkettbar.

Provider argumentieren meist, dass diese Profile nötig sind, um das Vertrauen in potenzielle Handelspartner und damit den Gewinn möglicher Interaktionen zu vergrößern. Aber der Aspekt der Gewinnmaximierung ist umstritten [Dellarocas 2003]. Dafür können geschickte Marketingexperten diese Informationen vergleichbar zu Empfehlungssystemen dazu nutzen, um nutzerspezifische Werbung zu generieren. eBay selbst macht sich dies bereits zu nutze, indem es Nutzern gezielt mit Empfehlungssystemen passende Produkte zu den bisherigen Einkäufen und Produktrecherchen anbietet.

4.7.3 (Un-)Verkettbarkeit und Reputation

Da nach der EU-Datenschutzrichtlinie 1995/46/EG „personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person“, gibt es juristische Argumente dafür, dass auch Meinungen über eine natürliche Person zu den personenbezogenen Daten gezählt werden sollten. Schon beim Design eines Reputationssystems, das Meinungen über natürliche Personen sammeln kann, sollten datenschutzrechtliche Anforderungen beachtet werden [Mahler/Olsen 2004]. Ein datenschutzfreundliches Reputationssystem [Steinbrecher 2006] erlaubt beispielsweise:

- *Parallele Verwendung von Pseudonymen:* Unverkettbarkeit zwischen Interaktionen in verschiedenen Kontexten (oder Kontexttypen), in die ein Nutzer eingebunden ist, kann durch Verwendung von Rollenpseudonymen bezüglich dieser Kontexte erreicht werden. Dies hat den positiven Nebeneffekt, dass Reputationen für unterschiedliche Rollen, die ein Nutzer in diesen unterschiedlichen Kontexten einnimmt, getrennt gesammelt werden. Dies sollte die Vertrauenswürdigkeit der Reputationssysteme erhöhen, da Nutzer abhängig vom Kontext unterschiedlich vertrauenswürdig sein können. Die Definition, was unter Kontext zu verstehen ist, bzw. die Unterscheidung zwischen verschiedenen Kontexten muss für das Reputationssystem gemacht werden, um die Reputationen, die unter einem Pseudonym gesammelt werden, für die anderen Nutzer sinnvoll auswertbar zu machen. Alle Nutzer mit Zugang zum Reputationssystem haben die Möglichkeit, die Kontextinformationen bezüglich dieses Pseudonyms zu verketten.
- *Terminierung der Nutzung eines Pseudonyms mit Reputationsübertragung auf ein anderes Pseudonym:* Nutzer sollten die Pseudonyme, die sie innerhalb eines Kontextes verwenden, von Zeit zu Zeit in der Form wechseln, dass sie ein altes Pseudonym ablegen und stattdessen ein neues verwenden. Dies gibt Mitgliedern die Möglichkeit, die Verkettbarkeit ihrer Handlungen innerhalb der Community zu bestimmen. Sie können auch ihre Reputation auf diesen neuen Pseudonymen weiterverwenden, wenn entsprechende Maßnahmen dies ermöglichen. Die Verwendung umrechenbarer Beglaubigungen (Credentials), die von einem Identitätstreuhänder ausgestellt werden, erlaubt es, Beglaubigungen, die zu einem seiner Pseudonyme gemacht werden, in Beglaubigungen zu einem anderen seiner Pseudonyme umzurechnen, während die Pseudonyme und die zugehörigen Beglaubigungen unverkettbar zueinander für jeden außer ihm selbst bleiben. Aber der Identitätstreuhänder kann im Falle eines Missbrauchs des Pseudonyms den zugehörigen Nutzer auf Anfrage aufdecken.

An das Reputationssystem werden zudem wiederum als informationstechnisches System mehrseitige Sicherheitsanforderungen gestellt. In der Regel sammeln Reputationssysteme im Sinne der semantischen Sicherheitsanforderungen nur Erfahrungen über das korrekte, nicht über das diskrete Verhalten von Nutzern, da der Zeithorizont von letzterem viel größer ist. Reputationssysteme könnten prinzipiell aber auch Informationen über Indiskretionen von Mitgliedern sammeln, und ein entsprechendes Fehlverhalten eines Mitglieds kann zum Ausschluss an der Community führen.

4.8 Metriken

Wie bereits in Abschnitt 4.1 festgestellt worden ist, gibt es im Wesentlichen zwei Ziele, die bezüglich einer Verkettung von Daten verfolgt werden:

1. die Kontrollierbarkeit von möglichen Verkettungen und
2. das Finden von Verkettungsmöglichkeiten in Datenbeständen.

Für beide Ziele kann der Grad der Zielerreichung mit Hilfe der Messung von Verkettbarkeit bzw. Unverkettbarkeit gem. [Pfitzmann/Hansen 2007] festgestellt werden.

Um eine Messung durchführen zu können, muss zunächst das System definiert werden, in dem gemessen werden soll. Eine solche Systemdefinition muss beinhalten:

- Eine Definition von Daten bzw. Ereignissen, deren Verkettbarkeit gemessen werden soll. In Bezug auf ein Kommunikationssystem, wie z.B. das Internet, können es Daten von Nutzern bestimmter Internetdienste im Internet sein. Weiterhin kann die Verkettbarkeit verschiedener Aktionen bezüglich eines Nutzers gemessen werden.
- Eine Definition des konkreten Schutzzieles, bzw. umgekehrt eine Definition des Angreifers. Diese Definition legt fest, welche Informationen für die Feststellung von Verkettbarkeit der Items of Interest (IOIs) zur Verfügung stehen. Dies können zum Beispiel die Informationen sein, die einem Dienstanbieter im Internet während der Nutzung des Dienstes durch verschiedene Nutzer bekannt werden. Im Bezug auf ein Schutzziel „Unverkettbarkeit“ kann man diese Informationen als dem Angreifer auf Unverkettbarkeit zur Verfügung stehende Informationen bezeichnen.

Das Ziel einer Messmethode ist es, herauszufinden, inwieweit die dem Angreifer zur Verfügung stehenden Informationen ausreichen, einen Zusammenhang zwischen den IOIs nachzuweisen.

Konkretere Systemdefinitionen hängen hierbei sowohl stark von dem zu betrachtenden System als auch von der anzuwendenden Messmethode ab.

4.8.1 Messmethoden für (Un-)Verkettbarkeit

Konkrete Messmethoden wurden bisher im Wesentlichen für die Bewertung von Anonymität, d.h. Unverkettbarkeit zwischen Nutzern und ihren von ihnen durchgeführten Aktionen (Anonymität in Kommunikationsnetzen) bzw. ihnen zugehörigen Datensätzen (Anonymität in statistischen Datenbanken), entwickelt.

4.8.1.1 Anonymität in Kommunikationsnetzen

Messmöglichkeiten für Verkettbarkeit bzw. Anonymität wurden im Wesentlichen für Proxy- und Mix-basierte Netze entwickelt, da diese die einzigen Netzkonzepte sind, die im größeren Stil in der Praxis eingesetzt werden.

Es wurden hierbei zwei Ansätze verfolgt. Einerseits wurde untersucht, wie sich Unverkettbarkeitseigenschaften mit Hilfe von formalen Sprachen und Logiken nachweisen lassen, und zum anderen wurden entropiebasierte Maße definiert.

Zur ersten Kategorie gehört z.B. ein Ansatz von Schneider und Sidiropoulos [Schneider/Sidiropoulos 1996], in dem die Modellierungssprache CSP für eine Formalisierung von Anonymitätseigenschaften verwendet wird. Einen ähnlichen Ansatz verfolgen auch Syverson und Stubblebine [Syverson/Stubblebine 1999], die formale Sprachen basierend auf Gruppenstrukturen zur Beschreibung von Anonymitätseigenschaften verwenden. Ein weiterer Ansatz von Hughes und Shmatikov [Hughes/Shmatikov 2004] definiert Verkettbarkeitseigenschaften anhand von Teilwissen über eine mathematische Funktion. Alle diese Ansätze haben gemein, dass jeweils nur possibilistische Aussagen gemacht werden können, d.h., es kann zwar gesagt werden, dass IOIs verkettbar sind oder nicht, aber es ist nicht möglich, Abstufungen bezüglich der Gewissheit der Verkettbarkeit zu ermitteln.

Ansätze der zweiten Kategorie gehen alle auf die Arbeit von Shannon [Shannon 1948], in der er die Entropie als eine Möglichkeit zum Messen des statistischen Informationsgehalts einer Informationsquelle definiert. Am Beispiel der Anonymität von möglichen Sendern einer Nachricht in Kommunikationsnetzen kann das folgendermaßen veranschaulicht werden: Alle potenziell möglichen Sender werden als Quellzeichen einer Informationsquelle aufgefasst. Durch Informationen, die über das Netz bzw. den Sendevorgang zur Verfügung stehen können unterschiedlichen Sendern unterschiedliche Wahrscheinlichkeiten zugewiesen werden, die angeben, mit welcher Sicherheit der jeweilige potenzielle Sender der tatsächliche Sender der Nachricht war. Anhand dieser Wahrscheinlichkeiten kann dann für die Quelle (potenzielle Sender mit zugeordneten Sendewahrscheinlichkeiten) eine Entropie berechnet werden. Diese gibt die (durchschnittliche) Ungewissheit an, die über den Sender der Nachricht besteht. Diese Ungewissheit kann wiederum durch die Größe einer Anonymitätsmenge ausgedrückt werden. Dieser Ansatz wurde sowohl von Serjantov und Danezis [Serjantov/Danezis 2002] als auch von Díaz et al. [Díaz et al. 2002] zum Messen von Anonymitätseigenschaften in Mix-basierten Netzen benutzt. Um die Dienstqualität eines Anonymisierungsdienstes zu bewerten, setzen Díaz et al. die ermittelte Anonymitätsmenge in Relation zur maximal möglichen Anonymität (d.h. der Menge aller möglichen Sender einer Nachricht).

In [Steinbrecher/Köpsell 2003] verallgemeinern Steinbrecher und Köpsell dieses Anonymitätsmaß zu einem Maß für Unverkettbarkeit, indem von Sendern, Empfängern und Nachrichten abstrahiert und allgemein die Verkettbarkeit zwischen Objekten bestimmt wird, die in einer bestimmten Relation zueinander stehen.

Die bisher einzige benutzbare Implementierung einer Anonymitätsmessung für Anonymisierungsdienste wurde im Rahmen des Projekts AN.ON entwickelt. Dabei wird aus der Anzahl der angemeldeten Nutzer des Dienstes, dem „Verkehrsaufkommen“ im Anonymisierungsdienst sowie der Anzahl der verwendeten Mixe in der verwendeten Mixkaskade ein Wert ermittelt, der dem Nutzer auf einer Skala angezeigt wird. Diese „Messung“ hat allerdings nicht den Anspruch, einen exakten Wert für die Anonymität zu bestimmen. Sie dient lediglich zur schnellen Orientierung des Nutzers bzw. zum Vergleich verschiedener angebotener Mixkaskaden. Abbildung 15 zeigt die Anonymitätsskala, die dem Nutzer angezeigt wird.

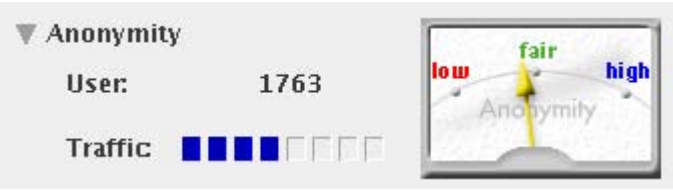


Abbildung 15: Anonymitätsskala von AN.ON

4.8.1.2 Anonymität in statistischen Datenbanken

In statistische Datenbanken werden Datensätze gespeichert, die u.a. personenbezogene Daten in einem bestimmten Kontext speichern, um daraus Statistiken abzuleiten. Beispielsweise kann eine Datenbank, die Daten über die Einwohner eines Ortes speichert, als statistische Datenbank angesehen werden.

Das Hauptziel bezüglich Unverkettbarkeit in statistischen Datenbanken ist es, dass zwar aussagekräftige Statistiken aus den gespeicherten Datensätzen abgeleitet werden können, es aber nicht möglich ist aus den Statistiken wiederum auf die Daten einer einzelnen Person (bzw. einer Gruppe von Personen unter einer festgelegten Gruppengröße) zu schließen. Dabei gibt es im Wesentlichen zwei Arten von Angriffen, bezüglich derer Unverkettbarkeit gewahrt bleiben soll:

1. *Angriffe durch den Betreiber der Datenbank:* Gegen diese kann vorgegangen werden, indem die Daten so auf verschiedene Betreiber aufgeteilt werden, dass Angriffe nur dann erfolgreich sind, wenn ein bestimmte Anzahl von Betreibern zusammenarbeiten.

2. *Angriffe durch Aggregation von Datenbankabfragen:* Hierbei werden aus der Datenbank erhaltene Statistiken mit anderen Statistiken bzw. mit außerhalb der Datenbank verfügbaren Informationen so verknüpft, dass daraus Informationen über einzelne Datensätze ableitbar sind. Solche Angriffen können erschwert werden, indem die Anfragemöglichkeiten für die Datenbank eingeschränkt werden, bzw. die Anfrageergebnisse so modifiziert werden, dass dies auf die gewünschten Statistiken einen minimalen Einfluss hat, aber die Zusammenführung zum Ermitteln einzelner Datensätze erschwert.

Eine detaillierte Beschreibung solcher Angriffe befindet sich u.a. in [Pommerening 1991] und [Paaß/Wauschkuhn 1984]. Gegenmaßnahmen werden in [Denning 1982] beschrieben.

Für die Messung von Anonymität in statistischen Datenbanken wird oft die so genannte *k*-Anonymität verwendet [Sweeney 2002]. Eine Datenbank sichert *k*-Anonymität zu, wenn sichergestellt ist, dass herausgegebene sensitive Daten immer jeweils *k* Individuen zugeordnet werden können.

Um die Größe von *k* zu bestimmen, gibt es verschiedene Ansätze. Sweeney benutzt hierfür einen possibilistischen Ansatz, der im Wesentlichen darauf basiert, dass zunächst festgelegt wird, welche Daten sensitiv bzw. nicht sensitiv sind. *k*-Anonymität wird gewährleistet, indem bei jeder Datenabfrage zunächst ermittelt wird, ob die herauszugebenden sensitiven Daten jeweils in mindestens *k* Datensätzen vorkommen. Wenn dies nicht der Fall ist, werden diese Daten nicht herausgegeben.

Ein Nachteil dieser Methode ist die Nichtbeachtung von gegenseitigen Abhängigkeiten zwischen Daten in der Datenbank. Ein Angreifer könnte solche Abhängigkeiten nutzen, um daraus wiederum auf einzelne Datensätze zu schließen. Fischer-Hübner ([Fischer-Hübner 2001, Section 4.1.2.2]) beschreibt dafür ein Maß für ein Risiko der Re-Identifikation, für dessen Berechnung sowohl bekannte statistische Abhängigkeiten zwischen verschiedenen Datenfeldern, als auch unterschiedliche Wahrscheinlichkeiten für verschiedene Werte eines Datenfeldes einbezogen werden. Dieses Maß basiert wie die oben beschriebenen probabilistischen Maße zur Messung von Anonymität in Kommunikationsnetzen auf der Berechnung von Entropien.

4.8.2 Messung von Unverkettbarkeit in Identitätsmanagementsystemen

4.8.2.1 Systemmodell und Angreifermodell

Um Anonymität und Unverkettbarkeit eines Nutzers ermitteln zu können, wird zunächst ein Systemmodell benötigt, das die Nutzer, deren personenbezogene Daten, sowie die Kommunikation zwischen den Beteiligten formal definiert. Weiterhin wird ein Angreifermodell benötigt, das festlegt, gegenüber welcher Art Angreifer Anonymität und Unverkettbarkeit gewährleistet bzw. gemessen werden soll.

Entsprechend dem Konzept des Identitätsmanagementsystems werden Informationen über einzelne Nutzer in Form von digitalen Identitäten definiert, die mehrere Attribute enthalten, wobei jedes Attribut wiederum einen Wert annehmen kann.

Das zugrundeliegende System wird folgendermaßen modelliert: Es existiert eine endliche Menge *E* von Nutzern. Die Nutzer haben Attribute, die zur Unterscheidung verschiedener Nutzer geeignet sind. Für jeden Nutzer existiert wenigstens eine Menge von Attributen, anhand derer er innerhalb der Menge aller Nutzer eindeutig identifiziert werden kann.

Eine Aktion besteht aus einer Kommunikation zwischen genau zwei Nutzern. Dabei übermittelt wenigstens einer der beiden Nutzer Attribute an den jeweils anderen. Es wird dabei angenommen, dass mehrere in einer Aktion übermittelte Attribute zusammengehören, das heißt, dass sie demselben Absender (Nutzer) zugeordnet werden können.

Ein Attribut wird als eine Menge von Attributwerten definiert, worin auch der Wert „nicht gesetzt“ enthalten ist. Im Modell wird eine endliche Menge von Attributen angenommen. Anhand der Attribute wird die digitale Identität als ein vollständiger Vektor von Attributwerten definiert. Eine digitale Identität enthält somit genau einen Wert jedes Attributs. Ein Nutzer kann eine oder mehrere digitale Identitäten haben.

Die in einem Identitätsmanagement tatsächlich verwendeten Attribute sind allerdings teilweise so gestaltet, dass sie explizit oder implizit Informationen über andere Attribute herausgeben. Beispielsweise sagt der Vorname in vielen Fällen etwas über das Geschlecht einer Person aus. Es muss also zunächst auch ermittelt werden, welche Attribute bei einer Aktion implizit übermittelt werden. Eine Methode zur Lösung dieses Problems wird in [Berthold/Clauß 2007] beschrieben.

Das Angreifermodell wird wie folgt beschrieben: Der Angreifer besteht aus einem oder mehreren Nutzern, mit denen andere Nutzer Aktionen durchführen. In Relation zu einem Nutzer *E* wird er wie folgt beschrieben: Der Angreifer kontrolliert einen oder mehrere Kommunikationspartner von *E*, das heißt, er erhält die von *E* mit diesen Kommunikationspartnern ausgetauschten Informationen (Attributwerte). Weiterhin stehen dem Angreifer zusätzliche Informationen über Attribute von Nutzern zur Verfügung, wie zum Beispiel Telefonbucheinträge oder Daten aus (öffentlichen) Statistiken.

4.8.2.2 Messen von Anonymität und Unverkettbarkeit

Es wird zunächst ein vermuteter konkreter Angreifer festgelegt. Eine Messinstanz versucht nun, die dem Angreifer vermutlich zur Verfügung stehenden Daten zu erhalten, und anhand dieser Daten Anonymität und Unverkettbarkeit von Aktionen eines Nutzers zu analysieren. In einem Privatheit fördernden Identitätsmanagementsystem könnte der Nutzer selbst eine solche Instanz sein, aber auch eine vertrauenswürdige dritte Partei.

Anhand des oben angegebenen Systemmodells wird ein formales Modell für die Aggregation von Informationen (Beobachtungen) in eine Informationsbasis definiert. Dieses beschreibt im Wesentlichen die Relationen zwischen den Auftrittshäufigkeiten der möglichen digitalen Identitäten, und die Änderung dieser Auftrittshäufigkeiten, wenn neue Beobachtungen aggregiert werden.

Das grundlegende Vorgehen beim Messen von Datenschutzeigenschaften anhand einer gegebenen Informationsbasis wird im Folgenden exemplarisch für das Schutzziel Anonymität beschrieben:

Da es um die Anonymität bezüglich einer Menge bereits herausgegebener bzw. noch herauszugebender Daten geht, werden diese Daten zunächst als Beobachtung formuliert. Aus der zugrundeliegenden Informationsbasis können nun die verdächtigen digitalen Identitäten bezüglich dieser Beobachtung extrahiert werden. Anhand dieser Verdächtigen und ihrer Wahrscheinlichkeiten kann nun die Shannon-Entropie berechnet werden. Diese gibt die Information in Bit an, die durchschnittlich zusätzlich benötigt wird, um die Beobachtung genau einer Identität zuzuordnen. Anschaulicher kann man diese Entropie auch als durchschnittliche Größe einer Anonymitätsmenge ansehen, in der alle Teilnehmer als gleich wahrscheinlich angenommen werden.

Falls die Informationsbasis Attribute enthält, die eine Zuordnung von digitalen Identitäten zu einzelnen Nutzern ermöglicht, kann Anonymität durch entsprechende Gruppierung der digitalen Identitäten auch für Nutzer berechnet werden.

Neben der durchschnittlichen Anonymität kann auch der Informationsgehalt einer bestimmten Identität (innerhalb der Menge der Verdächtigen) bestimmt werden. Dies gibt dann die Anonymität genau dieser Identität an. Da ein Nutzer oft seine digitale Identität(en) kennt, kann er damit seine persönliche Anonymität bestimmen. Weiterhin können die Extremwerte berechnet werden. Die untere Grenze ist dabei der Informationsgehalt der Identität mit der höchsten Wahrscheinlichkeit, während die obere Grenze die Anzahl der Verdächtigen ist.

Weiterhin stellt die Rényi-Entropie eine Möglichkeit zur Verfügung, mit Hilfe eines zusätzlichen Parameters einen bestimmten Punkt zwischen diesen Extremwerten der Entropie zu berechnen. Damit besteht die Möglichkeit eine Anonymitätsbestimmung an bestimmte Gegebenheiten eines konkreten Systems besser anzupassen.

Analog zur Anonymität kann Verkettbarkeit zweier Aktionen bestimmt werden, indem zunächst anhand der in den Aktionen herausgegebenen Daten zwei Verdächtigenmengen bestimmt werden. Anhand der Überschneidungen der Verdächtigenmengen und der Wahrscheinlichkeiten der verdächtigen Identitäten kann die Wahrscheinlichkeit, dass die Aktion von derselben Identität ausgeführt wurde, der Wahrscheinlichkeit gegenübergestellt werden, dass die Aktion nicht von derselben Identität ausgeführt wurde. Daraus erhält man einen Grad der Unverkettbarkeit.

4.8.2.3 Mehrseitige Sicherheit vs. Anonymitäts- und Verkettbarkeitsmessung

Ein wesentliches Ziel eines Privatheit fördernden, nutzergesteuerten Identitätsmanagementsystems ist es, dass die Nutzer bei der Benutzung von Diensten möglichst wenige personenbezogene Daten an möglichst wenige Instanzen herausgeben müssen. Andererseits ist es für eine aussagekräftige Bewertung von Anonymität und Unverkettbarkeit wichtig, dass der messenden Instanz möglichst viele Informationen über die Nutzer zur Verfügung stehen.

Wenn ein einzelner Nutzer seine Anonymität bzw. Unverkettbarkeit bewerten will, kann er seine personenbezogenen Daten am besten schützen, wenn er die Bewertung selbst vornimmt. Dafür benötigt er aber die personenbezogenen Daten sehr vieler anderer Nutzer, was wiederum für diese Nutzer ein Datenschutzproblem ist, da sie einem Nutzer, mit dem sie keinerlei Vertrauensverhältnis verbindet, sensible Daten mitteilen müssen. Somit ist die genaue Messung von Anonymität durch den Nutzer selbst aus Datenschutzgründen im Allgemeinen nicht durchführbar.

Es ist prinzipiell möglich die Bewertung von Anonymität und Unverkettbarkeit von einer dritten Partei durchführen zu lassen. Hierbei müssen allerdings geeignete Maßnahmen zur Gewährleistung der Korrektheit der Evaluationsergebnisse sowie Schutz der personenbezogenen Daten der Nutzer ergriffen werden.

Dem Problem der Korrektheit kann durch die Verwendung mehrerer unabhängiger Instanzen begegnet werden, indem eine Mehrheitsentscheidung über die Ergebnisse dieser Instanzen durchgeführt wird.

Neben juristischen Maßnahmen bezüglich Schadensersatz etc. können zum Schutz der Nutzerdaten Techniken eingesetzt werden, die eine Berechnung der Messergebnisse ermöglichen, ohne dass die berechnende Instanz Kenntnis von den der Berechnung zugrundeliegenden Daten erhält.

Hierfür gibt es zwei Ansätze: Zum einen können kryptographische Verfahren eingesetzt werden, die eine Berechnung sowie deren Eingaben und Ausgaben derart auf mehrere unabhängige Instanzen verteilen, dass jede einzelne Instanz anhand verschlüsselter Daten rechnet, aber das Endergebnis durch Zusammenführen der Teilergebnisse ermittelt werden kann. Solche Verfahren sind allerdings bisher sehr ineffizient, so dass sie für einen Einsatz bei einer an sich schon aufwändigen Berechnung nicht praktikabel sind. Zum anderen lässt sich die Berechnung in einer geschützten Umgebung durchführen, in der mittels physisch gesicherter Hardware und bezüglich Sicherheit verifizierter Software sichergestellt wird, dass die personenbezogenen Daten der Nutzer im geschützten Bereich verbleiben, also auch der Betreiber der Instanz nur Zugang zu den Berechnungsergebnissen erhält. Allerdings müssen die Nutzer auch hierbei dem Hersteller der sicheren Hardware vertrauen. Probleme liegen hier weiterhin bei der Sicherheitsverifikation der Software.

4.9 Ausgewählte Anwendungen

4.9.1 Erreichbarkeitsmanagement

Unter *Erreichbarkeitsmanagement* verstehen wir primär das Verwalten von Wünschen in Bezug auf telekommunikative Erreichbarkeit, d.h. das Erreicht-Werden z.B. per Festnetztelefon, Handy oder E-Mail. Der Begriff lässt sich ausdehnen auf ein Erreicht-Werden auf psychologischer Ebene beispielsweise durch zielgruppenspezifische Werbung, bei der der Empfänger nicht nur telekommunikativ erreicht wird, sondern der sie auch inhaltlich aufnimmt und sich vielleicht sogar emotional darauf einlässt.

Genauso wie vom Kontext abhängig ist, welche Daten man über sich preiszugeben willens ist, sind die Wünsche an die eigene telekommunikative Erreichbarkeit kontextspezifisch. Beispielsweise möchte man im Kino eigentlich nicht per Handy erreicht werden können, um den Film in Ruhe anzuschauen und auch die anderen Zuschauer nicht zu stören; im Notfall soll aber doch der Babysitteranruf durchgestellt werden. Oder der Chef soll (und will!) einen immer erreichen können, nicht aber im Urlaub oder in der Mittagspause.

Die telekommunikative Erreichbarkeit lässt sich in verschiedene Phasen zerlegen, was im Folgenden für einen Telefonanruf veranschaulicht wird:

1. Der Anrufer wählt die Nummer des gewünschten Kommunikationspartners und bringt damit zum Ausdruck, dass er diesen zu erreichen versucht.
2. Der Telekommunikationsbetreiber stellt diesen Verbindungsersuchen über sein Telekommunikationsnetz durch.
3. Das Endgerät des Angerufenen nimmt den Verbindungswunsch entgegen. Sofern dies nicht anders konfiguriert ist, klingelt das Telefon. Dabei lässt sich auch eine übertragende Rufnummer des Anrufers anzeigen. Einige Endgeräte speichern Informationen über Anrufversuche.
4. Ist der Angerufene anwesend, entscheidet er (z.B. anhand der übertragenden Rufnummer oder der Zeit des Anrufes), ob er den Anruf persönlich entgegen nimmt.
5. Wenn nein, lässt sich der Anruf auch auf einen Anrufbeantworter umleiten, von dem der Angerufene zu einem späteren Zeitpunkt Nachrichten abhören kann.

Man kann sicherlich diskutieren, ab wann „Erreichbarkeit“ in diesem Beispiel anfängt: Erst dann, wenn der Angerufene tatsächlich ans Telefon geht? Oder fiele auch die Aufzeichnung einer Nachricht durch den Anrufbeantworter hierunter – vielleicht erst, wenn die aufgenommene Nachricht durch den Angerufenen abgehört wird? Oder ist es schon die Übertragung der Rufnummer, die vom Angerufenen zur Kenntnis genommen wird, wodurch ihn die Tatsache des Verbindungswunsches erreicht? Spielt eine Rolle, ob die Aufmerksamkeit des Angerufenen auf den Verbindungsversuch gelenkt wird (was er als Störung seiner Privatsphäre empfinden kann)? Und soll der Angerufene eine Information darüber bekommen, inwieweit sein Verbindungswunsch beim Angerufenen angekommen ist?

All diese Facetten spielen eine Rolle beim Erreichbarkeitsmanagement. Aus Perspektive desjenigen, der erreicht werden soll, bedeutet dies die Konfiguration, inwieweit er für wen, ggf. auch zu welchen Zeiten, telekommunikativ erreichbar oder auch gerade nicht erreichbar sein möchte. Aus Perspektive desjenigen, der jemand anderes erreichen möchte, würde zum Erreichbarkeitsmanagement auch gehören, dass er ihn innerhalb bestimmter Rahmenbedingungen auch wirklich erreichen kann, z.B. dass über eine bestimmte Nummer auch eine Weiterleitung garantiert ist, wenn der Angerufene auf Reisen ist, oder dass ein Anruf zwischen 12 und 14 Uhr tatsächlich angenommen wird. Die individuellen Wünsche an ein Erreichen-Können und ein Erreicht-werden-Können müssen nicht übereinstimmen.

Neben organisatorischen Methoden wie z.B. dem Filtern der eingehenden Anrufe durch ein Vorzimmer, gibt es eine Reihe von technischen Methoden, die ein Erreichbarkeitsmanagement unterstützen (vgl. [Bertsch et al. 1995], [Rohwer et al. 2006]). Beispielsweise ermöglicht ein Wechsel von synchronen auf asynchrone Kommunikationskanäle (wie E-Mail, Fax, Umleiten auf eine Mailbox oder einen Anrufbeantworter), dass der zu Erreichende den Zeitpunkt bestimmen kann, wann er die Nachricht zur Kenntnis nimmt, und auch eine etwaige Antwort kann zeitverzögert kommen oder gar ausbleiben, was bei einem Telefonanruf zumindest Verwunderung auslösen würde. Anhand einer übertragenen Kennung des Kommunikationsinitiators, z.B. Absende-E-Mail-Adresse oder Rufnummer, kann man seine Reaktion bestimmen.

Einige Nutzer schützen sich recht erfolgreich vor Spam-E-Mails, indem sie nur bekannte Absenderadressen zulassen – allerdings müssen sich dann neue Kontakte erst bei ihnen auf anderem Wege registrieren, weil sie sonst nicht zu ihnen durchdringen können. Während in diesem Ansatz „White Lists“ mit zugelassenen Absendern verwendet wird, kann man in einigen Bereichen auch „Black Lists“ mit nicht-zugelassenen Kommunikationspartnern verwenden. Viele Handys bieten konfigurierbare Klingeltöne für einzelne Anrufer oder Anrufergruppen an, so dass der Angerufene anhand des Tons bestimmt, ob er den Anruf annimmt. Auch lassen sich Handys auf stumm oder vibrierend schalten, wenn Störungen gerade unerwünscht sind. Im Bereich von SPIT-Filtern (Spam over Internet Telephony) richten sich einige Maßnahmen speziell an Anrufmaschinen, die nicht in der Lage sind, eine Aufgabe (z.B. „Drücken Sie bitte 176#*“) oder ein anderes Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) zu lösen: Hier sollen Challenge-Response-

Tests, die für Menschen einfach, für Anrufmaschinen aber schwierig zu lösen sind, absolviert werden (vgl. [Rohwer et al. 2006]).

Da Erreichbarkeit wie auch die dafür nötige Kommunikation stets mehrere Beteiligte umfasst, können Aushandlungsprozesse für die Entscheidung, ob Kommunikationsversuche durchgestellt werden oder nicht, hilfreich sein. Bertsch et al. [Bertsch et al. 1995] schlagen die Implementierung von Erreichbarkeitsmanagern vor, bei denen sich die betroffenen Kommunikationspartner darüber verständigen, wie sie ihre Kommunikation gestalten wollen. Bei der Entscheidung können die kommunizierenden Personen (Name/Pseudonym, Funktion), der angegebene Gesprächsinhalt (Anlass oder Thema) oder die Kommunikationsumstände wie Ort oder Zeit Einfluss nehmen. Mitgesendete Referenzen anderer Personen können ebenso wie Angebote von Kautionen (digitales Geld, das der Angerufene behalten kann, wenn er sich gestört fühlt) vertrauensbildende Maßnahmen sein. Gerade die Idee der Geldübertragung zusammen mit der Nachricht ließe sich das Problem von E-Mail-Spam vermutlich schnell eindämmen.

Maßnahmen des Erreichbarkeitsmanagements können also das Verketten von Kommunikationsadressen zu der Person und zum Zugriff auf die Person als Kommunikationspartner unter Bedingungen stellen. Der Wunsch nach Konfiguration von Erreichbarkeit wird immer mehr Leuten bewusst, wenn sie gegen ihren Willen erreicht werden oder auch jemanden nicht erreichen können, obwohl sie glauben, dass diese Person unter den gegebenen Umständen hätte erreicht werden wollen. Daher werden vermutlich in nächster Zeit weitere Funktionen des Erreichbarkeitsmanagementkonzeptes von Bertsch et al. [Bertsch et al. 1995] in den Markt kommen.

4.9.2 Sichere elektronische Zahlungssysteme

In Abschnitt 3.3.2 zum Status Quo bei Zahlungssystemen wurden bereits Sicherheits- und Verkettbarkeitseigenschaften für Elektronische Zahlungssysteme vorgestellt. An dieser Stelle wird beispielhaft ein Zahlungssystem vorgestellt, das anonyme und unverkettbare Zahlungen ermöglicht.

Es wird zunächst angenommen, dass ein Benutzer *X* an einen anderen Benutzer *Y* des Zahlungssystems ein Recht transferieren möchte und ein Zeuge *B* (*B* für Bank) diesen Transfer bestätigt. Der Einfachheit halber soll von nur einem Zeugen ausgegangen werden. Dieser eine Zeuge soll für Falschzeugnisse haftbar sein: Das heißt, entstehen aufgrund seines Falschzeugnisses neue Rechte an Geld, so muss er dieses Geld bereitstellen, und weigert er sich, vorhandene Rechte zu bezeugen, so kann der davon Betroffene dies einem objektiven Dritten (z.B. einem Gericht) beweisen. Dies wird erreicht, indem dieser Zeuge finanziell hinreichend abgesichert und nicht anonym ist. Er übernimmt damit im Wesentlichen die Rolle einer Bank in herkömmlichen bargeldlosen Zahlungssystemen.

Man kann davon ausgehen, dass der Zahlende *X* und der Empfänger *Y* sich bereits unter gewissen Pseudonymen kennen. Diese Pseudonyme sind also von außerhalb des Zahlungssystems vorgegeben und werden als schützenswert betrachtet (im Allgemeinen Beziehungs- oder Rollenpseudonyme, z.B. Kundennummer und Bezeichnung eines Dienstanbieters). Ebenso vorgegeben ist das Pseudonym des Zeugen, der aber nicht anonym sein darf (öffentliches Personenpseudonym). Außerdem ist innerhalb des Zahlungssystems durch frühere Zahlungen bereits festgelegt, unter welchem Pseudonym *X* sich gegenüber dem Zeugen *B* als Inhaber des Rechts (des elektronischen Geldes), das er transferieren will, ausweisen kann. Seien also

pZ(X,t) das Pseudonym des Zahlenden *X* im Transfer *t* gegenüber dem Empfänger,

pE(Y,t) das Pseudonym des Empfängers *Y* im Transfer *t* gegenüber dem Zahlenden,

pB das für viele Zahlungen gleiche Pseudonym des Zeugen *B* und

pZB(X,t) das Pseudonym des Zahlenden *X* im Transfer *t* gegenüber dem Zeugen *B*.

Unter diesen Voraussetzungen ergeben sich, analog zu herkömmlichen Überweisungen, als Protokoll zum Transfer *t* des Rechts von *X* an *Y* die folgenden Ablaufschritte:

1. *Pseudonymwahl: Y* wählt sich ein Pseudonym *pEB(Y,t)*, unter dem er dem Zeugen *B* als Empfänger des Rechts im Transfer *t* bekannt sein möchte, und teilt *X* mit, dass er das Recht unter diesem Pseudonym *pEB(Y,t)* erhalten möchte. Entsprechend teilt *X* das Pseudonym

pZB(X,t), unter dem er das Recht transferieren will, *Y* mit. Die notwendigen Erklärungen sind mit *pE(Y,t)* bzw. *pZ(X,t)* authentisiert.

2. *Transferauftrag des Zahlenden: X* erteilt dem Zeugen *B* den Auftrag, das Recht an *pEB(Y,t)* zu übertragen. Dieser Auftrag ist mit *pZB(X,t)* signiert. Als Fremdauthentikation legt *X* diesem Auftrag eine Autorisierung bei, die besagt, dass *pZB(X,t)* über das zu transferierende Recht verfügt und von *B* selbst mit *pB* signiert ist. Da jeder Transfer von *B* beglaubigt sein muss, kann *B* nachprüfen, ob *pZB(X,t)* über das beglaubigte Recht tatsächlich noch verfügt oder es bereits transferiert wurde.
3. *Bestätigung des Zeugen:* Der Zeuge *B* bestätigt *X* und *Y* den Transfer des Rechts von *pZB(X,t)* auf *pEB(Y,t)*, wobei er sie unter diesen Pseudonymen adressiert.
4. *Quittung für den Zahlenden:* Der Empfänger *Y* sendet an *X* eine Quittung, die nur *pZ(X,t)* und *pE(Y,t)* bezeichnet und mit *pE(Y,t)* authentisiert ist und die den Erhalt des Rechts bestätigt. Verweigert *Y* die Quittung (was im Allgemeinen nicht zu verhindern ist, da *Y* anonym ist), so kann *X* die Bestätigung des Transfers durch *B* (aus [3]) zusammen mit der Bestätigung von *Y*, das Recht unter diesem neuen Pseudonym *pEB(Y,t)* empfangen zu wollen (aus Schritt 1), als Ersatzquittung verwenden.
5. *Bestätigung für den Empfänger:* Der Zahlende *X* sendet an *Y* eine Bestätigung des Transfers, die nur *pZ(X,t)* und *pE(Y,t)* bezeichnet und mit *pZ(X,t)* authentisiert ist. Auch *Y* kann notfalls die Bestätigung von *B* (aus Schritt 3) zusammen mit der Bestätigung von *X* (aus Schritt 1), das Recht an *Y* transferieren zu wollen, als Beweis dafür verwenden, das Recht von *pZ(X,t)* empfangen zu haben.
6. *Umformen der Bestätigung: Y* wird die auf *pEB(Y,t)* ausgestellte Bestätigung von *B*, das Recht erhalten zu haben, bei einem zukünftigen Transfer *t'* in Schritt 2 verwenden wollen. Um Verkettbarkeiten und damit mögliche Deanonymisierung zu vermeiden, sollte dort nicht *pEB(Y,t)* als *pZB(Y,t')* verwendet werden.

Durch Verwendung umrechenbarer Autorisierungen (z.B. [Chaum 1984a]) wird erreicht, dass *Y* die Bestätigung auf ein neues Pseudonym umrechnen kann. Dazu muss *Y* allerdings bereits in Schritt 1 des Transfers *t* zuerst das künftige Pseudonym *pZB(Y,t')* gewählt und daraus ein zur Umrechnung geeignetes *pEB(Y,t)* gebildet haben.

Abbildung 16 zeigt das Grundschema eines sicheren und anonymen digitalen Zahlungssystems.

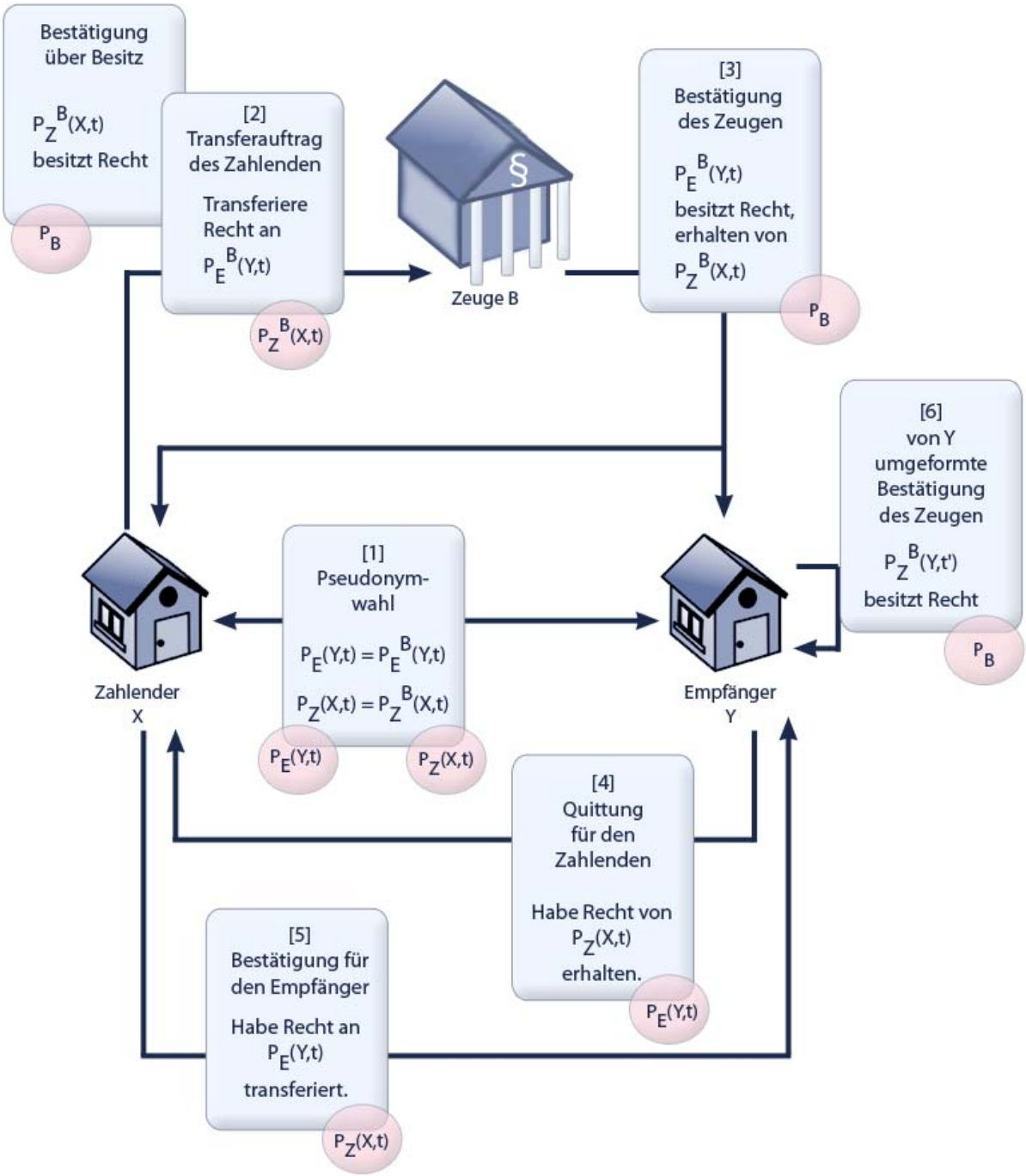


Abbildung 16: Grundschema eines sicheren und anonymen digitalen Zahlungssystems

Da man die in Schritt 6 erhaltene Bestätigung über den Empfang des Rechts in einem zukünftigen Transfer verwendet, um dasselbe Recht, d.h. denselben Geldbetrag, zu transferieren, ist es sinnvoll, in diesem Zahlungssystem wie bei Bargeld Rechte vorgegebener Nennwerte zu verwenden, aus denen man bei jeder Zahlung den gewünschten Betrag zusammensetzt. Natürlich muss man auch bei *B* Geld wechseln dürfen.

Damit man den umgeformten Bestätigungen bei ihrer Verwendung in Schritt 2 den Nennwert ansieht, verwendet *B* für jeden Nennwert *N* eine andere digitale Signatur, d.h. ein eigenes Pseudonym *pB,N*. Die Sicherheit des Protokolls ergibt sich daraus, dass am Ende eines Transfers jeder der drei

Beteiligten genügend Dokumente über dessen Stattfinden hat (die er aufbewahren muss) und auch während des Transfers jeder einem objektiven Dritten stets entweder den aktuellen Zustand beweisen oder diesen überprüfbar herstellen kann, indem er die bisher von anderen erhaltenen Nachrichten vorlegt und seine eigenen, sofern deren Erhalt abgestritten wird, noch einmal sendet. Außerdem können Forderungen innerhalb eines Transfers, die eingetrieben werden müssen, nur an den Zeugen entstehen, der nicht anonym ist.

Halten sich *X* und *Y* an das Protokoll, so ist die Anonymität des Protokolls maximal, da keiner durch den Transfer über einen anderen irgendwelche neue Information erhält: Der Zeuge erfährt bei einer Zahlung keines der Pseudonyme, die *X* und *Y* sonst verwenden, sondern nur zwei neue, die außer in dieser einen Zahlung nie mehr vorkommen. *X* und *Y* erfahren zwar voneinander auch die Pseudonyme, die sie bei dieser Zahlung gegenüber dem Zeugen verwenden, aber da diese mit nichts verkettbar sind und ohnehin klar war, dass irgendwelche Pseudonyme gegenüber dem Zeugen verwendet werden, stellt auch dies keine neue Information dar.

4.10 Technische Möglichkeiten zur Entkettung von Daten

Zur Betrachtung von technischen Möglichkeiten zum Entketten von Daten lassen sich zwei Konstellationen unterscheiden, die im Folgenden erläutert werden. Für jede dieser Konstellationen werden dann die technischen Entkettungsmöglichkeiten dargestellt.

Unabhängig von der Konstellation und den gewählten technischen Mechanismen ist die Information über eine gewünschte oder auch rechtlich geforderte (vgl. Abschnitt 2.3.3.2) Entkettung ein weiteres Datum, das in vielen Fällen sensibel ist und bei dem man nicht ausschließen kann, dass es wiederum gespeichert und mit den bereits vorhandenen Daten zusammengeführt wird.

4.10.1 Konstellation 1

Eine Instanz, die die Kontrolle über erfasste Daten hat, möchte diese so modifizieren, dass bestimmte Zusammenhänge nicht mehr erkennbar sind, d.h., dass die Daten entkettet werden.

Zur Entkettung von Daten gibt es hier grundsätzlich zwei Möglichkeiten:

1. Werden einzelne oder aggregierte Datensätze (z.B. Statistiken) aus der Menge der erfassten Daten extrahiert, wird jeweils überprüft, ob bzw. bis zu welchem Grad sich diese Daten einer einzelnen Person oder einer eng begrenzten Personengruppe zuordnen lassen. Abfragen werden entsprechend beschränkt oder ausgegebene Datensätze werden so verändert, dass sie zwar dem Zweck der Datenerhebung noch dienen können, aber eine Zuordnung zu einzelnen Personen nicht mehr möglich ist. Weitergehende Details hierzu finden sich im Abschnitt 4.8.1.2 zu statistischen Datenbanken.
2. Verschiedene Datenfelder aus den Datensätzen können zunächst auf unterschiedliche Datenbanken aufgeteilt werden, die möglichst unter der Kontrolle unterschiedlicher Instanzen stehen sollten. Um eine kontrollierte Zusammenführung dennoch zu ermöglichen, können die Daten pseudonymisiert werden, d.h., den einzelnen Datensätzen werden zufällig gewählte Pseudonyme zugeordnet. Eine Zusammenführung ist dann nur möglich, wenn jeweils der benötigte Anteil der Instanzen zusammenarbeitet.

4.10.2 Konstellation 2

Daten wurden an eine nicht vertrauenswürdige Instanz herausgegeben und sollen nun nachträglich entkettet werden.

- Im Allgemeinen ist es technisch nicht möglich, die Löschung bzw. Entkettung von einmal herausgegebenen Daten zu erzwingen. Wenn Daten einmal herausgegeben bzw. erfasst wurden, können sie prinzipiell beliebig lange gespeichert und kopiert werden.
- Es ist prinzipiell mit technischen Maßnahmen möglich, gegenüber Dritten nachzuweisen, dass ein Computersystem eine bestimmte zertifizierte Hardware und Software benutzt. So kann

eine an sich nicht vertrauenswürdige Instanz ein System zur Datenverarbeitung nutzen, das nachweislich Daten nur in einer bestimmten, evtl. vom Nutzer beschränkbaren Weise verarbeitet. Über diesen Mechanismus können Entkettungsmaßnahmen technisch auch bei nicht vertrauenswürdigen Instanzen durchgesetzt werden. Diese entsprechen dann im Wesentlichen den unter Konstellation 1 genannten Maßnahmen, wobei das Vertrauensverhältnis zur Daten erfassenden Instanz durch ein Vertrauensverhältnis zum Zertifizierer der Hard- und Software ersetzt wird. Eine solche Maßnahme kann aber nur eingesetzt werden, wenn entsprechend verifizierte Hard- und Software vorhanden ist. Des Weiteren muss es der entsprechende (Geschäfts-)Prozess, für den die Daten erhoben werden, zulassen, dass der bezüglich Verkettung kritische Anteil der Daten ausschließlich innerhalb des zertifizierten Systems verarbeitet werden kann. Insbesondere müssten diese Daten auch vor dem Zugriff nicht vertrauenswürdiger Administratoren geschützt sein. Aufgrund des technischen und organisatorischen Aufwands erscheint ein solches Vorgehen allenfalls in speziellen Fällen praktikabel.

- In bestimmten Fällen – insbesondere dann, wenn die Daten verarbeitende Instanz keine Gewissheit hat, dass die Daten korrekt und aktuell sind – kann durch das Hinzufügen von geeigneten Fehlinformationen ein vorhandenes Datenprofil unschärfer gemacht werden. Für eine gezielte Entkettung kann geplant Desinformation lanciert werden, oder aber es kann sich um versehentliche Missinformation handeln. Um eine echte Entkettung handelte es sich dann, wenn die betroffenen Daten tatsächlich nicht mehr verwendet werden können, z.B. weil der verarbeitenden Instanz bewusst wird, dass das ihr vorliegende Datenprofil – beispielsweise aufgrund von widersprüchlichen Informationen – unstimmig ist, und dann die entsprechenden Daten herauslöscht.
  Allerdings kann ebenfalls der Fall eintreten, dass mit den Fehlinformationen gearbeitet wird, was sich auf die Person auswirken kann, um deren Datenprofil es geht, oder aber auf andere Personen, die dann irrtümlicherweise mit falschen Informationen in Verbindung gebracht werden. Dann hätte die weitere Verkettung der ursprünglichen Daten mit Fehlinformationen keinen echten entkettenden Effekt.[476]

[476] Sofern andere Beziehungen aufgrund von Fehlinformationen hergestellt würden, könnte man von einer „Umkettung“ sprechen.

5 Szenarien

5.1 Einleitung

In den vorherigen Teilen dieser Arbeit sind die wesentlichen Begriffe zum Thema Verkettung erläutert und weitere Grundlagen vermittelt worden. Außerdem wurde ein Überblick über bereits bestehende Verkettungen in den Bereichen Bürger-Staat, Verbraucher-Unternehmen und Internet-Communities gegeben, um zu verdeutlichen, dass schon heute viele digitale Identitäten existieren und auch miteinander verkettet werden. Aufbauend auf den im Grundlagenteil vorgestellten technischen Grundlagen wurden schließlich vertiefende Informationen zu Techniken und Methoden von Verkettung vermittelt, um dem Leser ein besseres Verständnis von Zusammenhängen zu ermöglichen. In diesem Kapitel werden nun anhand von vier Szenarien einige aktuelle Themen und Entwicklungen näher beleuchtet, die im Hinblick auf eine Verkettung digitaler Identitäten als besonders wichtig und relevant für die Zukunft erscheinen.

Hierbei handelt es sich um:

- die zunehmende Verbreitung von Alltagsgegenständen, die eine Erhebung und Speicherung digitaler Daten und damit eine Verkettung digitaler Identitäten ermöglichen (z.B. Mobiltelefon oder MP3-Player) und die Tatsache, dass leistungsfähige Überwachungsgegenstände zu immer günstigeren Preisen angeboten und damit auch für Privatpersonen erschwinglich werden **(Szenario 1)**,
- die umfangreichen technischen Möglichkeiten zur Verkettung digitaler Identitäten, die daraus resultieren, dass verschiedene Unternehmen ihren Kunden eine Vielzahl an – personalisierten – Diensten (z.B. Suchmaschine, E-Mail-Konto und persönlicher Kalender) anbieten **(Szenario 2)**,
- die Möglichkeit einer Erstellung umfassender Bewegungsprofile von Personen anhand von Ortsdaten, die bei der Nutzung standortbezogener Dienste anfallen, und die Tatsache, dass ein solches Tracking technisch eine umfassende Überwachung von Personen – so beispielsweise die Überwachung von Arbeitnehmern durch den jeweiligen Arbeitgeber – ermöglicht **(Szenario 3)**, und
- die schier unbegrenzten Verkettungsmöglichkeiten, die die zunehmende Informatisierung unseres Alltags (Stichwort „Ubiquitous Computing“) mit sich bringt, und der Umstand, dass entsprechende Verkettungen aus Sicht des Betroffenen häufig unerwünscht, in vielen Fällen aber auch ausdrücklich erwünscht sein werden **(Szenario 4)**.

Innerhalb der einzelnen Szenarien finden sich jeweils die – aus dem Bereich der Kryptographie bekannten – Personen Alice und Bob, die vorliegend die durch Verkettung(en) Betroffenen darstellen.[477] Außer diesen beiden treten in den Szenarien auch noch weitere Beteiligte in Erscheinung, bei denen es sich überwiegend um die Instanzen handelt, die die jeweiligen Verkettungen vornehmen.

5.2 Szenario 1: Beobachtung und Verkettung durch Privatpersonen

5.2.1 Einleitung

Im Rahmen dieser Arbeit wurden vielerlei Fälle dargestellt, in denen staatliche und private Organisationen digitale Teilidentitäten von Personen sowie die dazugehörigen Datenbestände miteinander verketten. Allerdings hat schon das Kapitel zu Internet-Communities deutlich gemacht, dass auch Privatpersonen in zunehmendem Maße Verkettungen vornehmen können und dies auch tun.

[477] Szenario 1 bildet allerdings insoweit eine Ausnahme, weil dort nur Bob (potenziell) von einer Verkettung betroffen ist, Alice hingegen in diesem Szenario den Part des (potenziellen) Verketters übernimmt.

Die Thematik der Verkettung durch Privatpersonen wird im nachfolgenden Szenario erneut aufgegriffen und vertieft. Im Mittelpunkt steht dabei das Problem der Durchführung von Überwachungsmaßnahmen durch Privatpersonen. Verdeutlicht werden soll hier zum einen, wie einfach und kostengünstig man mittlerweile diese Überwachungstools wie Videokameras oder Minisender käuflich erwerben können. Zum anderen soll aber auch dafür sensibilisiert werden, dass es bereits eine Vielzahl von Alltagsgegenständen wie etwa Mobiltelefone, Webcams oder MP3-Player gibt, die sich auch zu Überwachungszwecken einsetzen lassen. Da die aus einer solchen Überwachung resultierenden Daten stets in digitaler Form anfallen, ist es ein Leichtes, sie im Nachhinein mit anderen digitalen Datenbeständen zu verketten.

5.2.2 Szenario

Alice und Bob sind seit einigen Jahren verheiratet. In letzter Zeit kommt Bob werktags oft erst spät von der Arbeit nach Hause und ist auch am Wochenende häufiger alleine unterwegs als sonst. Er erklärt dies Alice gegenüber damit, dass er gegenwärtig beruflich besonders viel zu tun habe und am Wochenende mehr Zeit für sich brauche, um den mit der vielen Arbeit verbundenen Stress abzubauen. Alice ist von dieser Erklärung nicht überzeugt und hat den Verdacht, dass Bob eine Affäre mit einer anderen Frau haben könnte. Außerdem gefällt ihr Bobs häufige und lange Abwesenheit auch deshalb nicht, weil sie seit einigen Tagen den Eindruck hat, dass ein ihr nicht bekannter Mann sich auffallend häufig in der Nähe ihrer Wohnung aufhält und diese beobachtet. Allerdings ist sie sich nicht ganz sicher, ob sie stets dieselbe Person in der Nähe des Hauses gesehen hat oder ob es sich nicht vielmehr um verschiedene Personen handelt, die einander einfach nur ähnlich sehen.

Alice überlegt, wie sie herausfinden kann, ob sie Bob zu Recht verdächtigt und ob die Wohnung tatsächlich von einer fremden Person beobachtet wird. Zunächst zieht sie in Betracht, einen Privatdetektiv zu engagieren. Als sie jedoch erfährt, mit welchen Kosten dies verbunden wäre, verwirft sie diesen Gedanken wieder. Eine Bekannte, der sie ihr Leid klagt, schlägt ihr vor, doch einfach selbst aktiv zu werden. Wenn Bob tatsächlich eine Geliebte habe, so sei doch damit zu rechnen, dass er zu dieser auch regelmäßig telefonisch Kontakt aufnehme. In diesem Fall müsse man damit rechnen, dass der intelligente Bob so vorsichtig wie möglich agiere. Es sei dann also wahrscheinlich, dass er für solche Telefonate nicht den Festnetzapparat nutze und die gewählte Rufnummer stets wieder aus dem Speicher seines Mobiltelefons entferne. Dies stelle aber kein Problem dar, da Alice doch ihre beiden Mobiltelefone dazu verwenden könne, Bob zu belauschen: Bevor sie beispielsweise am Wochenende das Haus verlasse, könne sie bei ihrem neuen Handy die Funktion der automatischen Rufannahme aktivieren und das Gerät etwa in Bobs Arbeitszimmer verstecken. Nach dem Verlassen der Wohnung könne sie dann von einem beliebigen Ort aus das neue Mobiltelefon mit ihrem alten Handy anrufen und so Telefonate, die Bob vom Arbeitszimmer aus führe, mithören. Wenn ihr diese Lösung zu teuer sein, könne sie stattdessen ihren MP3-Player mit Aufnahmefunktion im Arbeitszimmer deponieren und vor dem Verlassen des Hauses jeweils eine Aufnahme zu starten. Hinsichtlich des möglichen fremden Beobachters schlägt die Bekannte vor, Alice solle ihren Laptop samt Webcam auf dem Fensterbrett eines der zur Straße hinausgehenden Wohnungsfenster platzieren und das Geschehen auf der Straße mit Hilfe der Webcam einfach aufnehmen.

Wenn dies alles immer noch nicht ausreiche, um die beiden Sachverhalte aufzuklären, könne Alice dann noch im Internet professionelle Überwachungswerkzeuge bestellen. Solche Tools würden von einer Vielzahl von Anbietern offeriert, könnten bequem per Mausklick geordert werden und seien jedenfalls viel preiswerter als eine Detektei.

Alice ist sich nicht sicher, ob sie die Vorschläge der Bekannten tatsächlich in die Tat umsetzen soll. Der Gedanke, Bob nach zu spionieren, behagt ihr auf einmal doch nicht mehr. Auch hält sie es nach einigem Nachdenken für wahrscheinlich, dass sie sich die Existenz des fremden Beobachters nur eingebildet hat. Jedoch haben die Ausführungen der Bekannten ihre Neugier geweckt: Sie beschließt nachzuprüfen, ob im Internet tatsächlich eine große Auswahl an Überwachungswerkzeugen angeboten wird. Außerdem möchte sie zumindest einmal ausprobieren, ob sich die Mobiltelefone und die Webcam tatsächlich so einsetzen lassen, wie die Bekannte dies beschrieben hat.

5.2.3 Überblick über für Privatpersonen verfügbare Überwachungstools

Anknüpfend an das oben skizzierte Szenario wird nachfolgend ein Überblick darüber gegeben, welche Überwachungswerkzeuge heute von Privatpersonen zu erschwinglichen Preisen via Internet erworben werden können. Außerdem werden einige Alltagsgegenstände aufgelistet, die zu Überwachungszwecken eingesetzt werden können, auch wenn sie primär anderen Zwecken dienen.

5.2.3.1 Überblick über originäre Überwachungswerkzeuge

Bereits eine kurze Recherche im Internet offenbart, dass dort tatsächlich eine Vielzahl von Anbietern die unterschiedlichsten Überwachungswerkzeuge offeriert. Exemplarisch seien hier die folgenden Websites deutscher[478] Anbieter genannt:

- http://www.007spyshop.de/
- http://www.alarm.de/
- http://www.hiq-videosystems.de/
- http://www.provitek.de/
- http://www.solid-company.de/shop/
- http://www.spionagemarkt.de/
- http://www.spionage-ueberwachungstechnik.de/
- http://www.spiontechnik.de/
- http://www.topsicherheit.de/
- http://www.v-security.de/

Bei den Überwachungswerkzeugen, die via Internet erworben werden können, wird vorliegend zwischen Tools zur Audio-, Video-, Telefon- und PC-Überwachung unterschieden[479].

5.2.3.1.1 Werkzeuge zur Audioüberwachung

Mit Werkzeugen zur Audioüberwachung können vertrauliche Gespräche belauscht und zumeist auch aufgezeichnet werden. Es wird zwischen Audio-Recordern, Minisendern und Geräten zur Geräuschverstärkung und/oder -filterung differenziert.

Audio-Recorder ermöglichen das heimliche Aufzeichnen vertraulicher Gespräche. Die meisten der oben genannten Anbieter führen eine Vielzahl solcher Recorder in ihrem Sortiment. So wird beispielsweise ein digitaler Audio-Recorder mit mehr als 18 Stunden Aufnahmekapazität und automatischem Stopp bei Sprechpausen bereits für 50 EUR angeboten. Für 195 EUR ist sogar schon ein digitaler Recorder mit einer Aufnahmekapazität von nahezu 12 Tagen erhältlich, der folglich auch zur Langzeitüberwachung geeignet ist[480].

Die umgangssprachlich als Wanzen bezeichneten Minisender ermöglichen zusammen mit den entsprechenden Empfangsgeräten eine drahtlose Geräuschüberwachung. Diese Sender sind so klein, dass sie sich leicht in einem Raum verstecken lassen. Im Übrigen enthalten die meisten der Empfangsgeräte Anschlussmöglichkeiten für Audio-Recorder, so dass Gespräche dann auch gleich

[478] Beispiele für Websites ausländischer Anbieter sind etwa http://spyville.com/ (letzter Zugriff im Oktober 2007), http://www.spyzone.com/ (letzter Zugriff im Oktober 2007) und http://www.spygadgets.com/ (letzter Zugriff im Oktober 2007).

[479] Die nachfolgend unter Angabe des Preises genannten Beispielsprodukte wurden am 18. Mai 2007 auf der Webseite eines der oben genannten Anbieter zu den jeweils genannten Konditionen für den deutschen Markt offeriert.

[480] Im Übrigen können mit diesem Gerät, das mit einem entsprechenden Adapter mitgeliefert wird, auch Telefonate mitgeschnitten werden.

aufgenommen werden können. Auch solche leistungsfähigen Minisender nebst Empfangsgeräten sind zu Preisen erhältlich, die auch für durchschnittliche Privatpersonen erschwinglich sind. So wird etwa ein Set aus einem digitalen Minisender und einem Digitalempfänger mit einer Reichweite von 700 bis 2.000 Metern zu einem Preis von weniger als 400 EUR angeboten.

Geräte zur Geräuschverstärkung und -filterung ermöglichen es, auch leise oder weiter entfernt geführte Unterhaltungen zu belauschen, bestimmte Geräusche zu verstärken sowie unerwünschte Nebengeräusche zu eliminieren bzw. zu dämpfen. Beispielsweise[481] sollen sog. Richtmikrofone nur die Schallwellen, die aus der mit dem Mikrofon anvisierten Richtung kommen, erfassen. Auch hier können selbst sehr leistungsfähige Geräte schon zu niedrigen Preisen erworben werden. Ein Richtmikrofon mit elektronischem Geräuschverstärkungssystem, einer integrierten Zieloptik mit zehnfacher Vergrößerung und einem eingebauten 12 Sekunden-Recorder wird etwa für weniger als 60 EUR angeboten. Soll eine längere Aufzeichnung vorgenommen werden, kann auch hier ein externer Recorder an das Gerät angeschlossen werden.

5.2.3.1.2 Werkzeuge zur Videoüberwachung

Das wichtigste Werkzeug zur Videoüberwachung ist die sog. Überwachungskamera. Hierbei handelt es sich um eine – zumeist fest montierte – Videokamera, die dazu verwendet wird, ein Objekt oder einen räumlichen Bereich dauerhaft zu überwachen. Eine vollständige Videoüberwachungsanlage, auch CCTV-System[482] genannt, besteht immer zumindest aus einer solchen Kamera und einem damit verbundenen Anzeigegerät.

Es wird zwischen Kabel-, Funk und IP-Kameras differenziert[483]. Manche Systeme zeigen lediglich live ein Bild an, andere können dieses zwecks späterer Auswertung auch aufzeichnen. Neben Kameras, die nur Bilder übertragen können, gibt es solche, die gleichzeitig auch eine Übertragung von Tönen ermöglichen. Darüber hinaus lassen sich Farb- und Schwarzweiß- sowie Innen- und Außenkameras unterscheiden.

Besonders gut zu Überwachungszwecken geeignet sind getarnte Kameras. Hierbei handelt es sich um sehr kleine Exemplare, die als Gebrauchsgegenstände getarnt werden oder in solchen Gegenständen verborgen sind.

Auch Überwachungskameras werden wie die bereits vorgestellten Geräte zur Audioüberwachung schon zu vergleichsweise niedrigen Preisen angeboten. So kann etwa eine drahtlose Minikamera mit eingebautem Mikrofon, die Bilder und Töne aufnehmen und über eine Distanz von bis zu 200 Metern an ein beliebiges Anzeigegerät funken kann, bereits für weniger als 150 EUR käuflich erworben werden. Eine wetterfeste Nachtsicht-Kamera mit Zoomfunktion und einstellbarem Blickwinkel kostet mit ca. 180 EUR nur wenig mehr. Zu ähnlichen Preisen sind bei den oben genannten Anbietern auch schon entsprechende Anzeige- oder Aufnahmegeräte erhältlich.

Getarnte Kameras können beispielsweise in Kugelschreibern, Uhren, Sonnenbrillen, Handtaschen, Stofftieren oder Ventilatoren eingebaut werden. So wird etwa bei der sog. Teddycam eine Miniaturkamera in der Nase eines Teddybären versteckt. Die Übertragung zu dem dazugehörigen Empfänger erfolgt via Funk bei einer Reichweite von bis zu 250 Metern – ein eingebautes Mikrofon gehört ebenfalls zum Lieferumfang. Die Teddycam wird bereits zu einem Preis von 250 EUR angeboten[484].

Schließlich ist davon auszugehen, dass in einigen Jahren auch kleine fliegende Überwachungskameras (sog. Drohnen), die lange Zeit Kunden aus dem militärischen Umfeld vorbehalten waren, für Privatpersonen erschwinglich sein werden. Seit Juni 2006 verkauft beispielsweise das deutsche

[481] Außerdem sind hier auch sog. Stethoskope zu nennen, die zum Abhören von Wänden verwendet werden können.

[482] CCTV steht für Closed Circuit TeleVision.

[483] Letztere werden an bereits bestehende TCP/IP-Netze angeschlossen und können deshalb einfach und kostengünstig installiert werden.

[484] Bereits hier sei darauf hingewiesen, dass Vertrieb und Besitz einer solchen Funk-Teddycam und anderer getarnter Sendeanlagen in Deutschland nach dem Telekommunikationsgesetz strafbar sind. Für Mobiltelefone gilt dies hingegen nicht.

Unternehmen microdones GmbH[485] eine solche Drohne zu einem Preis von ca. 10.000 EUR[486]. Diese fliegende Überwachungskamera wird von vier Rotoren angetrieben und mittels eines GPS-Systems gesteuert. Sie ist 20 bis 30 km/h schnell, kann mit Hilfe des mitgelieferten Akkus bis zu 20 Minuten in der Luft bleiben und bis zu 200 g schwere Gegenstände wie etwa eine moderne Digitalkamera transportieren. Die Drohne ermöglicht es folglich, hochaufgelöste Luftbilder aufzunehmen – dies natürlich nicht nur von öffentlichen Gebäuden, sondern auch von Privatgrundstücken. Es scheint also nur eine Frage der Zeit zu sein, bis Privatpersonen solche fliegenden Kameras beispielsweise dazu benutzen werden, die Grundstücke ihrer Nachbarn oder von Prominenten zu erkunden.

5.2.3.1.3 Werkzeuge zur Telefonüberwachung

Werkzeuge zur Telefonüberwachung ermöglichen das Mitschneiden von Telefongesprächen. Gängige Geräte werden überwiegend direkt an der Telefonbuchse angeschlossen[487] und erlauben es, die an dem jeweiligen Telefonanschluss geführten Gespräche (heimlich) aufzuzeichnen. Vielfach wird hierzu nicht mehr ein separates Aufnahmegerät verwendet, sondern etwa mittels eines USB-Adapters die Möglichkeit geschaffen, Gespräche direkt auf der Festplatte eines PCs zu speichern.

Dabei wird ein einfacher Telefon-Recorder, der Telefongespräche digital bis zu einer Dauer von vier Stunden aufzeichnen kann, schon zu einem Preis von weniger als 120 EUR angeboten. Die getätigten Aufzeichnungen können von diesem Gerät auf einen externen Datenträger übertragen und dort auf Dauer gespeichert werden. USB-Mitschnittsysteme, die eine Speicherung von Telefonaten direkt auf dem PC ermöglichen, sind bereits zu Preisen von ca. 350 EUR erhältlich. Mit im Lieferumfang enthalten ist bei solchen Geräten zumeist noch eine spezielle Software, dies es u.a. ermöglicht, die gespeicherten Telefonate nach Kriterien wie Telefonnummer des Gesprächspartners oder Datum und Uhrzeit des Anrufs zu durchsuchen. Schließlich sind leistungsfähige Mitschnittsysteme für komplette ISDN[488]-Anschlüsse, die ebenfalls eine Aufzeichnung am PC ermöglichen, bereits zu Preisen von weniger als 600 EUR erhältlich[489].

5.2.3.1.4 Werkzeuge zur PC-Überwachung

Computer lassen sich mit Hilfe einschlägiger Programme (sog. Computer Monitoring Software) vollständig überwachen. Entsprechende Tools arbeiten unbemerkt im Hintergrund und kontrollieren, protokollieren und speichern sämtliche Aktivitäten, die auf dem jeweiligen PC stattfinden. So erfassen solche Programme insbesondere jeden Tastenanschlag, jede gestartete Anwendung, jede aufgerufene Webseite sowie jede geschriebene E-Mail. Auch können in frei definierbaren Zeitabständen Screenshots des gesamten Bildschirms aufgenommen werden. Ist der jeweilige PC mit einer Webcam ausgestattet, so besteht vielfach auch die Möglichkeit, automatisch Fotografien des aktuellen Benutzers anzufertigen. Zu den Features gehört darüber hinaus bei manchen Programmen der Versand detaillierter Nutzungsberichte des jeweiligen PCs an eine beliebige E-Mail-Adresse.

---

485 http://www.microdrones.com/ (letzter Zugriff im Oktober 2007).

486 Siehe den Artikel „Drohne für jedermann – mal sehen, was der Nachbar treibt“ bei SPIEGEL ONLINE, abrufbar unter http://www.spiegel.de/netzwelt/spielzeug/0,1518,456942,00.html (letzter Zugriff im Oktober 2007).

487 Bei einfacheren Lösungen wird ein Mikrofon am Mobilteil des Telefons angebracht. Solche Geräte lassen sich auch dazu verwenden, per Mobiltelefon geführte Gespräche aufzuzeichnen.

488 ISDN steht für Integrated Services Digital Network und ist ein internationaler Standard für ein digitales Telekommunikationsnetz.

489 Umfangreiche Informationen zu Schwachstellen in ISDN-Geräten hat der Chaos Computer Club auf seiner „Chaos-CD Blue“ (http://www.ccc.de/chaoscd/) zusammengestellt. Diese sind abrufbar unter http://www.trust-us.ch/isdn_dipl/002.html (letzter Zugriff im Oktober 2007). Dort findet sich auch ein Abschnitt zum Abhören von Telefongesprächen.

Professionelle Monitoring-Software ist oft schon für weniger als 50 (z.B. Orwell Monitoring[490]) bzw. 100 EUR (z.B. Spector Pro[491]) erhältlich, manche Monitoring-Tools werden sogar als Free- oder Shareware angeboten (z.B. PC Monitoring[492]).

5.2.3.2 Überblick über „überwachungstaugliche“ Alltagsgegenstände

Wie bereits das obige Szenario deutlich gemacht hat, gibt es neben solchen Werkzeugen, deren primärer Verwendungszweck in der Überwachung anderer Personen besteht, auch alltägliche Gebrauchsgegenstände, die eigentlich einem anderen Zweck dienen, aber auch zur Überwachung eingesetzt werden können.

Hierzu zählen etwa moderne Mobiltelefone mit eingebauter Digitalkamera (sog. Fotohandys), mit denen neben Bildern vielfach auch Töne und Videos aufgezeichnet werden können. Primärer Verwendungszweck dieser Geräte ist das mobile Telefonieren, gleichzeitig können sie aber auch als Fotoapparat, Diktiergerät oder Videokamera verwendet werden. Diese Funktionalitäten können natürlich nicht nur offen, sondern auch verdeckt zu Zwecken der Überwachung eingesetzt werden. Ähnliches gilt beispielsweise auch für Webcams, MP3-Player mit Aufnahmefunktion, Diktiergeräte, Babyphones und Anrufbeantworter.

Hinsichtlich dieser Geräte besteht allein aufgrund ihrer weiten Verbreitung innerhalb der Bevölkerung ein großes Risiko, dass sie auch zu Überwachungszwecken eingesetzt werden. Dies gilt insbesondere für Mobiltelefone: Schon heute kommen auf 100 Einwohner rund 105 Verträge und Prepaid-Karten – es gibt also in Deutschland bereits mehr Mobilfunkanschlüsse als Bürger[493]. Außerdem mögen viele Menschen Hemmungen haben, spezifische Überwachungsgeräte zu erwerben. Bei Alltagsgegenständen, die zunächst aus ganz anderen Gründen angeschafft werden, könnte aber wieder einmal der Spruch „Gelegenheit macht Diebe“ zutreffen: Man denke nur an das oben genannte Szenario und die dort angedeutete Eifersuchtsproblematik. Schon jetzt lässt sich im Übrigen feststellen, dass gerade in Schulen Mobilfunktelefone zweckentfremdet werden. So findet sich im Internet eine Vielzahl an mit Handys aufgenommenen Filmen, deren Inhalt von voyeuristischen Aufnahmen über Misshandlungen bis hin zu Vergewaltigungen reicht[494].

Schließlich sei an dieser Stelle noch einmal auf getarnte Überwachungswerkzeuge hingewiesen, die so als Alltagsgegenstand getarnt bzw. in solchen Gegenständen versteckt werden, dass sie in ihrer Funktion als Überwachungstool nicht ohne weiteres wahrgenommen werden können.

5.2.4 Rechtliche Aspekte: Einschlägige Straftatbestände

Heimliche Überwachungsmaßnahmen können für denjenigen, der sie vornimmt, sowohl zivil- als auch strafrechtliche Konsequenzen haben. Nachfolgend wird nur auf letztere eingegangen und dargestellt, welche Straftatbestände insoweit in Betracht kommen.

5.2.4.1 Verletzung der Vertraulichkeit des Wortes

Schutzgegenstand des § 201 Strafgesetzbuch (StGB)[495] ist das nichtöffentlich gesprochene Wort eines anderen. Strafbar macht sich zum einen, wer unbefugt – also gegen den Willen des Betroffenen – dessen nichtöffentlich gesprochenes Wort auf einen Tonträger aufnimmt oder eine solchermaßen hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht. Zum anderen wird aber auch

490 http://www.protectcom.de/ (letzter Zugriff im Oktober 2007).
491 http://www.spectorsoft.com/ (letzter Zugriff im Oktober 2007).
492 Vgl. etwa unter http://www.freeware-archiv.de/shareware/PCMonitoring-Ueberwachung.htm (letzter Zugriff im Oktober 2007).
493 Vgl. hierzu die letzte einschlägige Meldung des BITKOM vom März 2007, abrufbar unter http://www.bitkom.org/46624_44673.aspx (letzter Zugriff im Oktober 2007).
494 Informationen zum sog. Cyber-Bulling finden sich in dem Artikel „Von Schülern verhöhnt – und die ganze Welt sieht zu“ bei SPIEGEL ONLINE, der abrufbar ist unter http://www.spiegel.de/schulspiegel/0,1518,475897,00.html (letzter Zugriff im Oktober 2007).
495 Einzelheiten zu dieser Vorschrift finden sich etwa bei [Hoppe 2004].

bestraft, wer das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder das zuvor aufgenommene oder abgehörte Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

§ 201 StGB schützt den Einzelnen also insbesondere davor, dass seine vertraulich gemachten Äußerungen abgehört, aufgenommen und anderen zur Kenntnis gebracht werden. Wer dennoch unbefugt vertrauliche Gespräche belauscht oder aufzeichnet, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Die Tat wird im Übrigen nur auf Antrag des Belauschten verfolgt.

5.2.4.2 Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

Schutzgegenstand des § 201a StGB ist das aufgenommene Bild einer anderen Person. Strafbar nach dieser Norm macht sich, wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt. Ebenfalls strafbar ist es, eine solchermaßen hergestellte Bildaufnahme zu gebrauchen oder einem Dritten zugänglich zu machen. Schließlich erfasst diese Vorschrift auch die Fälle, in denen eine befugt hergestellte Bildaufnahme wissentlich unbefugt einem Dritten zugänglich gemacht wird.

§ 201a StGB ist im Jahre 2004 neu in das Strafgesetzbuch eingefügt worden und ergänzt die Strafnorm des § 33 Kunsturhebergesetz (KUG). Die Vorschrift erfüllt Forderungen nach einer strafrechtlichen Gleichstellung von unbefugtem Abhören und Abbilden. Konkreter Anlass für die Schaffung dieses neuen Straftatbestands war das Aufkommen neuer technischer Geräte wie Digitalkameras, Fotohandys oder Webcams.

Von § 201a geschützt wird nur, wer sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet. Beispiele für einen solchen geschützten Raum sind Toiletten, Umkleidekabinen oder ärztliche Behandlungszimmer. Des Weiteren muss durch das unbefugte Herstellen von Bildaufnahmen der höchstpersönliche Lebensbereich verletzt werden. Dies ist jedenfalls dann der Fall, wenn die betreffende Aufnahme Krankheit, Tod oder Sexualität abbildet. Wichtigster Anwendungsfall der Norm dürfte aber die Anfertigung von Nacktbildern sein. Neben entsprechenden Aufnahmen einer Person in ihrer Wohnung werden u.a. auch solche bei der Benutzung von Umkleidekabinen, Toiletten oder Saunen von § 201a StGB erfasst.

Ein Verstoß gegen diese Vorschrift wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Auch hier wird die Tat nur auf Antrag des Verletzten hin verfolgt.

5.2.4.3 Verbreiten oder öffentliches Zurschaustellen eines Bildnisses ohne Einwilligung

Neben § 201a StGB wird das Bild einer Person strafrechtlich auch durch § 33 Kunsturhebergesetz (KUG) geschützt. Hiernach ist das Verbreiten oder öffentliche Zurschaustellen eines Bildnisses ohne Einwilligung des Abgebildeten strafbar. Allerdings erfasst diese Norm nicht schon das bloße Herstellen einer Bildaufnahme[496], das nur unter den Voraussetzungen des bereits vorgestellten § 201a StGB strafrechtlich geschützt wird. Auch hier lautet die Strafandrohung auf bis zu einem Jahr Freiheitsstrafe oder Geldstrafe. Die Tat wird ebenfalls nur auf Antrag des Verletzten verfolgt.

5.2.4.4 Missbrauch von Sendeanlagen

§ 148 i.V.m. § 90 Telekommunikationsgesetz (TKG) stellen den Missbrauch von Sendeanlagen unter Strafe. Konkret geht es um getarnte Sendeanlagen wie die bereits weiter oben erwähnte Teddycam. Schutzgegenstand der genannten Normen sind das informationelle Selbstbestimmungsrecht und das Allgemeine Persönlichkeitsrecht. Strafbar macht sich nach § 148 Abs. 1 Nr. 2 TKG, wer entgegen § 90 Abs. 1 Satz 1 TKG eine dort genannte Sendeanlage besitzt. Gleiches gilt für den, der eine solche

[496] Gleiches gilt für das Übertragen und Gebrauchen einer Bildaufnahme.

Sendeanlage herstellt, vertreibt, einführt oder sonst in den Geltungsbereich des Gesetzes verbringt[497]. § 148 TKG selbst enthält damit also nur eine Strafandrohung und verweist hinsichtlich der tatbestandlichen Voraussetzungen größtenteils auf § 90 TKG[498].

Sendeanlagen im Sinne des § 90 TKG sind elektrische Sende- oder Empfangseinrichtungen, zwischen denen die Informationsübertragung ohne Verbindungsleitungen stattfinden kann. Erfasst werden Funkanlagen, die sowohl senden als auch empfangen, nicht jedoch reine Empfangsgeräte. Des Weiteren muss die jeweilige Sendeanlage ihrer Form nach einen anderen Gegenstand vortäuschen oder mit Gegenständen des täglichen Gebrauchs verkleidet sein und auf Grund dieser Umstände in besonderer Weise dazu geeignet sein, das nichtöffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen.

§ 148 TKG stellt bereits den Besitz solcher Anlagen unter Strafe – die Strafbarkeitsgrenze wird durch diese Bestimmungen also gegenüber den bereits vorgestellten Straftatbeständen weiter nach vorne verlagert. Ein weiterer Unterschied zu den bereits vorgestellten Vorschriften besteht darin, dass hier kein Strafantrag gestellt werden muss, sondern die Tat von Amts wegen verfolgt wird (sog. Offizialdelikt). Die Strafandrohung lautet auf bis zu zwei Jahre Freiheitsstrafe oder auf Geldstrafe.

5.2.5 Fazit

Das in diesem Abschnitt vorgestellte Szenario 1 macht deutlich, wie leicht Überwachungstools für jedermann einsetzbar sind. Selbst sehr leistungsfähige Werkzeuge können mittlerweile bequem via Internet und zu vergleichsweise geringen Preisen bestellt werden. Mit Hilfe solcher Tools können dritte Personen heimlich fotografiert oder gefilmt werden, des Weiteren können nichtöffentliche Gespräche belauscht und aufgezeichnet werden. Ein noch größeres Gefahrenpotenzial folgt allerdings aus bereits in großer Anzahl vorhandenen Alltagsgegenständen wie Mobiltelefon oder MP3-Player, die auch zu Überwachungszwecken eingesetzt werden können.

Da es sich bei den im Rahmen solcher Überwachungsmaßnahmen anfallenden Daten zumeist um digitale Daten handelt, können diese ohne weiteres mit anderen digitalen Informationen über die betroffene Person, über die der Überwachende verfügt, verkettet werden. Für den Betroffenen sind solche Verkettungen völlig intransparent, da er in der Regel schon gar nicht realisieren wird, dass er fotografiert, abgehört oder gefilmt wird.

5.3 Szenario 2: Verkettbarkeit bei der Nutzung von Diensten der Google Inc.

5.3.1 Dienste der Google Inc.

Die Firma Google Inc. ist der größte Suchmaschinenbetreiber der Welt. Die Zugriffe werden wie in Abschnitt 3.3.6 dargestellt zu Marketingzwecken verkettet. Zu Google Inc. gehört neben der Suchmaschine eine Vielzahl weiterer Dienste mit eigenen Datenspeicherungen, so z.B.:

- Google-Suche: jedes Suchwort, das ein Nutzer bei Google eingibt;
- Goolge-Desktop: ein Index der Computerdateien eines Nutzers einschließlich der E-Mails, der Musik, Fotos und der Chat- und Webbrowser-Historie;
- Google-Talk: Instant-Message-Chats zwischen Nutzern;
- Google-Maps: erfragte geographische Adressen und Routen, oft inklusive der Wohnadresse des Nutzers, um Richtungen anzuzeigen;
- Google-Mail (Gmail): E-Mail-Historie eines Nutzers mit der Voreinstellung, E-Mails „für immer“ zu speichern;

[497] Insoweit wird nach § 148 Abs. 2 TKG auch ein fahrlässiges Handeln unter Strafe gestellt.
[498] Es handelt sich bei dieser Vorschrift also um einen sog. Blankettstraftatbestand.

- Google-Calendar: Terminplan eines Nutzers, wie er vom Nutzer eingegeben wird;
- Google-Orkut: Tool für Social Networking, das persönliche Informationen speichert wie Name, Wohnort, Status der Beziehung usw.;
- Google-Reader: ATOM/RSS-Feeds, die ein Nutzer liest;
- Google Video/YouTube: Videos, die sich ein Nutzer anschaut;
- Google-Checkout: Kreditkarten- oder Zahlungsinformationen zur Benutzung auf anderen Webseiten.

Im März 2007 hat Google Inc. das Unternehmen DoubleClick Inc. erworben. DoubleClick Inc. vermarktet Werbung durch zielgerichtete Schaltung von Anzeigen im Internet (*„targeted advertising“*).

Nachfolgend beschreibt ein fiktives Beispiel, das sich an den technischen Möglichkeiten von Google Inc. orientiert, welche Verknüpfung von digitalen Identitäten hier existieren. Voranzustellen ist dabei, dass zwischen der technisch möglichen Verknüpfung und der rechtlich zulässigen Verknüpfung zu unterscheiden ist. In dem nachfolgenden Szenario wird auf die Verkettungsmöglichkeiten im Bereich der Datenbestände und Systeme der Google Inc. eingegangen. Die Frage der rechtlichen Zulässigkeit oder der tatsächlichen Praxis wurde dabei bewusst außer Acht gelassen, um technische Potenziale für Verkettung in den Vordergrund der Betrachtung zu rücken.

5.3.2 Verkettung von Datenbeständen bei der Fa. DoubleClick

DoubleClick ist Hersteller einer Software, die zur Vermarktung von Werbung Internet eingesetzt wird (DART-Produktreihe). Sie unterhält Kooperationsverträge mit Werbetreibenden und Werbevertriebsfirmen. Auf den Seiten, die Werbung unter Nutzung der Software der Firma DoubleClick einblenden, wird ein Cookie der DoubleClick bezogen und auf dem aufrufenden Computer gespeichert. Hierdurch erhält DoubleClick die Information, unter welcher IP-Adresse eine bestimmte Internetseite zu welcher Zeit aufgerufen wird. Durch Verkettung dieser Adressen kann so ein umfangreiches Surf- und somit Interessensprofil erstellt werden. Durch den Cookie ist es möglich, den Nutzer verschiedener Internet-Sessions wiederzuerkennen. Dieses Interessensprofil lässt sich weiter verdichten, indem es mit den bei Google verfügbaren Suchanfragen über die Vergleichsattribute IP-Adresse und Zeitraum verknüpft wird. Der Umfang dieses Profils hängt dabei maßgeblich davon ab, wie stark der Nutzer Seiten frequentiert, die mit DoubleClick kooperieren, und inwieweit er google.com als Suchmaschine nutzt.

Derzeit unterhält DoubleClick Kooperationsverträge zu einer Reihe von Werbevermarktern in Deutschland und weltweit, so z.B. die TOMORROW FOCUS AG[499], die eine Reichweite von 32,6 % der Internetnutzer hat[500]. Zu den von ihnen mit Werbung beschalteten Seiten zählen unter anderem Amica Online, Focus Online, Playboy.de und Map24.com. Daneben weisen die über den Vermarkter AdLINK Internet Media GmbH mit Werbung beschalteten Seiten einen DoubleClick-Cookie auf[501]. Über die AdLINK Internet Media GmbH wird eine Vielzahl der Internetauftritte von Tageszeitungen (so z.B. Berliner Zeitung, WAZ, Hamburger Morgenpost, u.a.[502]) mit Werbung beschickt.

5.3.3 Beispielszenario

Möglichkeiten und Grenzen der Verkettung der Datenbestände bei den von Google Inc. angebotenen Diensten sollen nachfolgend anhand zweier fiktiver Szenarien dargestellt werden. Ausdrücklich wird erneut darauf hingewiesen, dass nicht behauptet werden soll, dass die Google Inc. ein derartiges Profil erstellt; das Beispiel soll lediglich die Aktionsmöglichkeiten erläutern.

[499] http://www.slazenger.de/pb/detail/Doubleclick_und_die_TOMORROW_FOCUS_AG_weiten_Zusammenarbeit_aus.html (letzter Zugriff im Oktober 2007).
[500] AGOF e.V., Internet Facts 2006-IV.
[501] Stichprobentest der Verfasser.
[502] AGOF e.V., Internet Facts 2006-IV.

5.3.3.1 Nutzung von Google Inc.-Diensten durch Bob

Bob, 31, Informatiker. Bob ist kritischer Computernutzer. Er nutzt Anonymisierungsdienste beim Surfen und lässt sich, um Profilbildung zu vermeiden, regelmäßig eine neue IP-Adresse zuweisen. Er schließt damit aus, dass eine Verkettung seines Nutzungsverhaltens über längere Zeiträume möglich ist. Cookies hat er deaktiviert, die Speicherung gestattet er nur in solchen Ausnahmefällen, in denen er sich davon überzeugt hat, dass dies in seinem Interesse liegt. In Einzelfällen sieht Bob davon ab, das Internet zu benutzen, weil er nicht überblicken kann, welche Daten dabei entstehen.

Bei Bob ergeben sich ohne weiteres keine Möglichkeiten zur Bildung umfangreicher Profile und Verkettungen. Abfolgen von Suchanfragen, bei denen er keine zwischenzeitliche Erneuerung der IP-Adresse durch den Anonymisierungsdienst vornehmen lässt, lassen sich allerdings dennoch zusammenführen. Sein Surfverhalten kann auch nicht über Cookies verkettet werden. Allerdings kann er eine Verkettung über sog. Web-Bugs[503] mit seinem Verhalten nicht ausschließen.

Bei Web-Bugs werden kleine – für den Nutzer nicht auffällige – Graphiken in Webseiten von deren Betreiber integriert. Diese Graphiken stammen jedoch nicht vom Betreiber selbst, sondern von dritter Seite und werden von dort herunter geladen, so dass dort jedes Mal, wenn ein Internetangebot eines Partners aufgerufen wird, auch eine Datenspur in Form der IP-Adresse des Nutzers entsteht. Über diese IP-Adresse lässt sich wiederum das Verhalten des Nutzers über die verschiedenen Angebote verfolgen.

5.3.3.2 Nutzung von Google Inc.-Diensten durch Alice

Alice, 26, ist Studentin und arbeitet an einer Masterarbeit zur Entwicklungszusammenarbeit. Abends liest sie oft ihre private E-Mail und chattet über Gmail, einem Dienst der Google Inc. Dass dabei Werbung korrespondierend zum Inhalt ihrer E-Mail geschaltet wird, empfindet sie als praktisch. Auch die Suchmaschine nutzt sie intensiv. Webseiten, die sie aufsucht, findet sie oft leichter über Suchbegriffe bei google.com, als sich die Domainnamen zu merken. Hierdurch entstehen auch Spuren über die von ihr aufgesuchten Internetangebote. Tabelle 16 zeigt eine Sammlung von Einträgen, die sich in den Logfiles der jeweiligen Dienste befinden könnten:

[503] Auch „Web Beacon“, „Clear GIF“ oder „Pixel-Tags“ genannt.

Uhrzeit	Eintrag
18.30.10	gmail.com: Anmeldung unter dem Benutzernamen Alice1981
18.31.23	gmail.com: Aufruf diverser E-Mails
19.15.11	google.de, Eingabe der Suchanfrage: entwicklungshilfeorganisationen jobs
19.16.33	google.de, Eingabe der Suchanfrage: auswärtiges amt jobs
19.16.38	google.de: Anwahl des ersten Suchtreffers in der Liste: Auswärtiges Amt-Tätigkeit bei internationalen Organisationen
anschließend	Surfen auf den Seiten des Auswärtigen Amtes
19.22.38	Erneute Anmeldung bei gmail.com
19.23.12	gmail.com: Mail verfassen angeklickt
19.27.49	Besuch der Internetseite travelchannel.de
19.29.22	travelchannel.de: Anwahl des Angebotes für Pauschalreisen unter 300 EUR
19.31.12	travelchannel.de: Anwahl des Angebotes für Luxusreisen
19.32.30	travelchannel.de: Anwahl eines Angebotes für die französische Mittelmeerküste
19.33.21	travelchannel.de: Erneutes Laden des Angebotes für Luxusreisen
19.34.12	travelchannel.de: Anwahl des Angebotes für Reisen nach Afrika
19.35.43	travelchannel.de: Anwahl des Angebotes für Tansania/Sansibar
19.36.12	travelchannel.de: Anwahl des Angebotes für den Breezes Beach Club von Meiers Weltreisen
19.41.12	google.de: Suchanfrage: Sansibar virtualtourist
anschließend	Surfen auf den Seiten von virtualtourist.com
20.12.14	gmail.com: E-Mail verschicken an kip@auswaertiges-amt.de mit folgendem Betreff: Anmeldung Karrieremesse und dem Text: „Sehr geehrter Herr …“
20.13.01	amica.de: Anwahl der Seite: Seite Kuss-Check
20.41.02	Erneute Anmeldung bei Gmail
20.43.12	gmail.de: Chat mit Nutzerin Alicia1980 mit folgendem Inhalt: „Hey Alicia …“
21.33.12	Abmeldung bei Gmail

Tabelle 16: Logfile von Alice

In Tabelle 16 ist eine Sammlung von Einträgen dargestellt, die sich – in technisch standardisierter Form (vorliegend wurden sie zum Zwecke der Lesbarkeit in Stichpunkte übersetzt und vereinfacht) – in den Logfiles der jeweiligen Dienste befinden könnten. Sämtliche der oben bezeichneten Suchanfragen, Seitenaufrufe oder anderen Aktionen lassen sich untereinander und zu einem einzigen Profil verketten. Die dazu erforderlichen Daten liegen alle zumindest während der Erbringung des jeweiligen Dienstes in einem technischen System, über das Google Inc. aufgrund seiner Beteiligungen die Kontrolle hat. Die Webseiten travelchannel.de und Amica.de nutzen DoubleClick und hinterlassen entsprechende Cookies. Eine Verkettung wäre jeweils über Zeitstempel und IP-Adresse oder über die Verknüpfung von Cookies möglich. Lediglich das Surfverhalten auf den Seiten des Auswärtigen Amtes und bei virtualtourist.com ist nicht offensichtlich für Google Inc. nachverfolgbar.

Die Auswertungsmöglichkeiten der oben dargestellten Profile sind vielfältig. So stellen [Hu et al. 2007] in einem kürzlich veröffentlichten Papier dar, wie das Geschlecht und Altersgruppe eines Nutzers aus dem Surfverhalten abgeleitet werden kann.

Typische Auswertungsverfahren umfassen vor allen Dingen die Aggregierung der Datenbestände und zielen nicht nur auf Profilbildung ab. In der Kombination mit den im Vorangegangenen dargestellten Auswertungsmöglichkeiten der individuellen Daten zum demographischen Hintergrund eines Nutzers lässt sich Werbung zielgruppenorientiert präsentieren. Während zielgruppengerechte Schaltung von Werbung kein Novum darstellt, sind die Möglichkeiten der Erfassung der Verhaltensweisen, die dann – unter Umständen – letztlich bis zu einer Kauf eines Produktes führen, in der nunmehr möglichen Dichte bemerkenswert.

So können Verfahren entwickelt werden, die Aussagen treffen, wie hoch die statistische Wahrscheinlichkeit, dass der Nutzer einem Werbelink folgt, und die abgeleitet von den vorhandenen individuellen Nutzercharakteristika sind. Die Genauigkeit statistischer Verfahren bestimmt sich maßgeblich aus dem sog. Hebesatz, also der Anzahl der erfassten Personen und Entscheidungen. Es kann mittels der vorgestellten Möglichkeiten sehr viel genauer prognostiziert werden, wie spezifische Verhaltensweisen bei bestimmten Einflüssen gesteuert werden, da der Prognose nahezu eine Vollerhebung des Nutzerverhaltens zugrunde liegt.

5.3.4 Fazit

Eine detaillierte rechtliche Prüfung der oben dargestellten Szenarien würde den Rahmen dieser Arbeit sprengen. Eine solche an dieser Stelle vorzunehmen, ist auch nicht sinnvoll, da mit Beispielen gearbeitet wurde, die eben gerade nicht beanspruchen, die tatsächliche Praxis abzubilden, sondern lediglich technische Möglichkeiten erläutern sollten.

Auffällig ist jedoch aus rechtlicher Sicht, dass auch ohne dass ein Personenbezug im Sinne des BDSG vorliegt, das dem Datenschutzrecht zugrundeliegende Schutzziel betroffen ist. Selbst wenn Alice im Einzelfall nicht individualisierbar ist, d.h. Google Inc. (oder auch Dritte) aus dem Profil nicht die natürliche Person ableiten können, droht doch die Gefahr eines erheblichen Informationsungleichgewichts zwischen den Parteien. Alice kann nicht überblicken, was die Gegenseite über sie weiß, und dieser Informationsvorsprung kann auch zur Verhaltensbeeinflussung genutzt werden.

Bobs Verhalten, die Nutzung bestimmter Dienste zu vermeiden, ist daher nachvollziehbar. Ob sich derartige Einflussnahmen in relevanter Zahl tatsächlich darstellen oder darzustellen drohen, bedürfte allerdings einer empirischen Untersuchung. Festgestellt werden kann jedoch, dass eine solche Verhaltensanpassung zu verhindern erklärtes Ziel des Datenschutzes ist. Das Bundesverfassungsgericht legte in seinem Volkszählungsurteil dar: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. (…) Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“ (BVerfGE 65,1).

5.4 Szenario 3: Location Based Services – Tracking am Arbeitsplatz

5.4.1 Allgemeines zu Location Based Services

5.4.1.1 Überblick

Als *Location Based Services (LBS)* werden Dienstleistungen bezeichnet, die dem Nutzer mittels mobiler elektronischer Kommunikationstechniken zur Verfügung gestellt und in Abhängigkeit von

seinem aktuellen Standort erbracht werden. Um dem Nutzer gegen Zahlung eines Entgelts einen Mehrwert zur Verfügung stellen zu können, kombinieren solche standortbezogenen Dienste Daten über den aktuellen Aufenthaltsort eines Gerätes – und damit auch über den Aufenthaltsort der Person, die dieses Gerät mit sich führt – mit anderen Informationen.[504]

Mittlerweile wird eine Vielzahl unterschiedlicher standortbezogener Dienste angeboten: So werden etwa Navigationsdienste offeriert, die für den Nutzer die Berechnung der jeweils günstigsten Route zu seinem Zielort übernehmen und hierfür u.U. auch aktuelle Verkehrsinformationen berücksichtigen. Des Weiteren gibt es verschiedene Varianten sog. Informationsdienste, die den Nutzer z.B. darüber unterrichten, welche Restaurants, Apotheken, Kinos oder Sehenswürdigkeiten sich in seiner Nähe befinden. Darüber hinaus lässt sich unter Zuhilfenahme sog. „Buddy-Finder"-Dienste herausfinden, wo sich Verwandte oder Freunde gerade aufhalten. „Tracking"-Dienste ermöglichen es, die Position einer Person, eines Fahrzeugs oder eines Produkts zu verfolgen: Mit ihrer Hilfe kann also beispielsweise festgestellt werden, wo sich die einzelnen Fahrzeuge eine Kraftfahrzeugflotte gerade befinden – hier liegen dann automatisch auch Informationen über den Aufenthaltsort des jeweiligen Fahrers vor. Die Funktion sog. Notfalldienste besteht hingegen darin, Rettungskräfte unverzüglich über die aktuelle Position einer verunglückten Person zu informieren. Weitere Beispiele für Location Based Services sind Dienste zur automatischen Einbuchung von Straßenbenutzungsgebühren („Mautgebühren") oder zur Ermöglichung ortsbezogener Werbung.

In begrifflicher Hinsicht lassen sich „Push"- und „Pull"-Dienste unterscheiden:[505] Charakteristisch für sog. „Push"-Dienste ist, dass die jeweilige Dienstleistung erfolgt, ohne dass der Nutzer dies initiiert hat. Der konkrete Dienst wird dem Nutzer also quasi von außen aufgedrängt. Dies ist beispielsweise bei einem Dienst der Fall, der dem Nutzer (unaufgefordert) ortsbezogene Werbung zukommen lässt. Bei sog. „Pull"-Diensten wird die entsprechende Dienstleistung hingegen nur dann zur Verfügung gestellt, wenn der Nutzer diese zuvor aktiv nachgefragt hat. Dies ist etwa bei vom Nutzer initiierten ortsbezogenen Suchanfragen der Fall. Im Übrigen lassen sich „Pull"-Dienste danach unterscheiden, ob auf die Anfrage des Nutzers hin nur eine einzelne Antwort des Dienstes erfolgt oder ob dieser nachfolgend so lange ortsbezogene Informationen übermittelt, bis eine bestimmte Bedingung eintritt.

5.4.1.2 Voraussetzungen für die Erbringung standortbezogener Dienste

Die Erbringung standortbezogener Dienste setzt zunächst voraus, dass die Position des jeweiligen mobilen Endgeräts bestimmt werden kann. Zu unterscheiden sind in diesem Zusammenhang netzbasierte und terminalbasierte Verfahren[506]: Netzbasierte Verfahren machen sich den Umstand zunutze, dass ein Funknetz die aktuelle Position eines Endgerätes bestimmen kann. So wird bei vielen ortsbezogenen Diensten die Position des Nutzers mit Hilfe der Daten über die Funkzelle, in der sich sein Mobiltelefon gerade befindet, bestimmt – dieses Ortungsverfahren nennt sich *„Cell of Origin"* oder kurz *Cell-ID*.[507] Bei netzbasierten Verfahren wird die Ortung also von dem jeweiligen Mobilfunkanbieter und nicht von dem Nutzer selbst vorgenommen. Dagegen erfolgt die Lokalisierung bei terminalbasierten Verfahren wie dem satellitengestützten *Global Positioning System (GPS)* mit Hilfe des mobilen Endgeräts und kann damit vom Nutzer des Dienstes kontrolliert werden.[508] In diesem Zusammenhang unterscheidet man die Begriffe *Tracking* (das mobile Endgerät wird geortet) und *Positioning* (das mobile Endgerät ortet sich selbst).

Zur Erbringung eines standortbezogenen Dienstes werden in der Regel nicht nur die aktuellen Positionsdaten des Nutzers, sondern darüber hinaus weitere Daten benötigt, ohne die der jeweilige Mehrwert für den Nutzer nicht generiert werden könnte. Dies können zum einen Daten über den Nutzer (z.B. zu seinen Hobbys und Interessen) sein, zum anderen kann es sich aber auch um bestimmte ortsbezogene Informationen handeln. Insoweit kann zwischen statischen und dynamischen

[504] Ein Überblick zu Location Based Services findet sich bei [TAUCIS 2006]. Ausführlichere Informationen (in englischer Sprache) stellen etwa [Steininger/Neun/Edwardes 2006] zur Verfügung.
[505] Hierzu vgl. etwa [TAUCIS 2006, S. 38].
[506] Zu den einzelnen insoweit gebräuchlichen Verfahren vgl. [Steininger/Neun/Edwardes 2006, S. 20 f.].
[507] Ein weiteres netzbasiertes Ortungsverfahren ist das sog. Time-of-Arrival-Verfahren (TOA).
[508] Als weiteres terminalbasiertes Ortungsverfahren ist das Enhanced Observed Time Difference-Verfahren (E-OTD) zu nennen, das auf dem Prinzip der Triangulation basiert.

Informationen differenziert werden[509]: Statische Informationen sind solche, die über einen gewissen Zeitraum hinweg konstant bleiben und beispielsweise – elektronischen – Branchenbüchern entnommen werden können. Bei dynamischen Informationen handelt es sich hingegen um solche, die sich innerhalb kurzer Zeit ändern können. Als Beispiele seien hier Hinweise zur Verkehrslage oder zum (lokalen) Wetter genannt. In vielen Fällen wird der Diensteanbieter nicht selbst über alle diese Informationen verfügen, sondern zumindest einen Teil seinerseits von einem Anbieter solcher Inhalte (einem sog. Content-Provider) beziehen.

Die Anforderung standortbezogener Dienstleistungen und die Übermittlung der jeweils generierten Informationen an den Nutzer erfolgt in den meisten Fällen über das Kommunikationsnetz eines Mobilfunkanbieters. Das hierfür benötigte mobile Endgerät kann mit dem Gerät, mittels dessen die Position des Nutzers ermittelt wird, identisch sein. Dies ist etwa dann der Fall, wenn zur Lokalisierung und zur Informationsübermittlung ein (GPS-)Mobiltelefon verwendet wird.

Zusammenfassend lässt sich sagen, dass für die Erbringung standortbezogener Dienste ein mobiles Endgerät, ein Kommunikationsnetz, ein Gerät zur Positionsbestimmung sowie ergänzende Informationen benötigt werden. Damit gibt es bei der Erbringung standortbezogener Dienste die folgenden Beteiligten:

- Nutzer des Location Based Services;
- lokalisiertes Subjekt bzw. Objekt[510];
- Betreiber des zur Datenübermittlung verwendeten Kommunikationsnetzes;
- Positionsermittler (z.B. Mobilfunkanbieter[511]);
- Anbieter des standortbezogenen Dienstes (LBS-Provider);
- Anbieter zusätzlicher Informationen (Content-Provider)[512].

5.4.2 Szenario: Tracking am Arbeitsplatz

5.4.2.1 Allgemeines zum Tracking von Personen oder Objekten

Wie bereits erwähnt, können standortbezogene Dienste zum Ziel haben, eine Person, ein Fahrzeug oder ein bestimmtes Produkt zu „tracken“, d.h. in regelmäßigen Abständen und über einen längeren Zeitraum hinweg den jeweiligen Aufenthaltsort zu bestimmen. Will etwa ein Unternehmen jederzeit wissen können, wo sich seine auszuliefernden Waren gerade befinden, so kann dies mittels eines *Trackings* aller Paketsendungen realisiert werden. Ebenso kann durch das Nachverfolgen der Positionsdaten aller Kraftfahrzeuge eines Fuhrparks ein effektives Flottenmanagement ermöglicht werden, das Disponenten die – aufeinander abgestimmte – Planung und Steuerung des Einsatzes der einzelnen Fahrzeuge erleichtert. Schließlich lässt sich mittels eines solchen Dienstes der Aufenthaltsort von (Service-)Mitarbeitern ermitteln, wodurch diese besonders effizient eingesetzt werden können – so kann beispielsweise bei einer neuen Kundenanfrage ein Mitarbeiter mit dieser betraut werden, der sich ohnehin schon räumlich in der Nähe des anfragenden Kunden befindet.

509 Hierzu [Steininger/Neun/Edwardes 2006, S. 7 f.].
510 Dieses wird oftmals mit dem Nutzer identisch sein.
511 Häufig wird dem Mobilfunkanbieter eine Doppelfunktion als Betreiber des Kommunikationsnetzes und als Positionsermittler zukommen.
512 Auch wenn bei der Erbringung von Location Based Services in vielen Fällen neben dem Diensteanbieter noch ein Content-Provider involviert ist, gibt es auch Konstellationen, in denen der Diensteanbieter selbst schon über alle notwendigen Informationen verfügt und deshalb die Mitwirkung eines Content-Providers nicht erforderlich ist.

5.4.2.2 Tracking eines Lastkraftwagens und des jeweiligen Fahrers

Das nachfolgende Szenario beschreibt eine Konstellation, in der ein LKW und damit auch dessen Fahrer(in) durch ein privates Unternehmen getrackt werden[513]:

In diesem Szenario wird ein Mobiltelefon mit eingebautem GPS-Empfänger in einem Lastkraftwagen installiert, um stets den aktuellen Aufenthaltsort des Fahrzeugs, das unterschiedliche Ziele innerhalb Europas ansteuert, ermitteln zu können. Fahrerin des LKW, der zum Fuhrpark der Verkettungs-Logistik AG (VL-AG) gehört, ist Alice, die auch bei diesem Unternehmen beschäftigt ist. Die jeweiligen Positionsdaten werden in regelmäßigen Abständen von einem zentralen Server der VL-AG abgerufen und anschließend in einer Datenbank gespeichert. Anhand dieser Daten lässt sich also nicht nur der aktuelle Aufenthaltsort des LKW bestimmen, sondern es kann auch nachvollzogen werden, an welchen Orten sich das Fahrzeug zu einem bestimmten Zeitpunkt in der Vergangenheit befunden hat. Ergeben sich – in örtlicher und/oder zeitlicher Hinsicht – signifikante Abweichungen zwischen dem Aufenthaltsort des LKW und der zuvor geplanten Route, so wird Alice durch einen anderen Mitarbeiter der VL-AG kontaktiert, der sie nach dem Grund für die jeweiligen Diskrepanzen fragt und sodann mit ihr mögliche Modifikationen der bisher gewählten Route diskutiert. Die Positionsdaten und die von Alice zusätzlich gemachten Angaben – etwa zur Verkehrssituation – werden zur weiteren Planung der Route verwendet. Die Positionsdaten ermöglichen es darüber hinaus, Bewegungsprofile von Alice zu erstellen und sie in ihrer Funktion als Fahrerin des Lastkraftwagens zu überwachen. So können mit Hilfe der Positionsdaten beispielsweise Pausenzeiten oder Durchschnittsgeschwindigkeiten des LKW nachvollzogen werden.

Abbildung 17 verdeutlicht den Ablauf des skizzierten Tracking-Dienstes.

[513] Ein thematisch verwandtes Szenario inklusive einer rechtlichen Analyse findet sich bei [Roßnagel et al. 2006, S. 63 ff. (Szenariobeschreibung) und S. 100 ff. (rechtliche Analyse)].

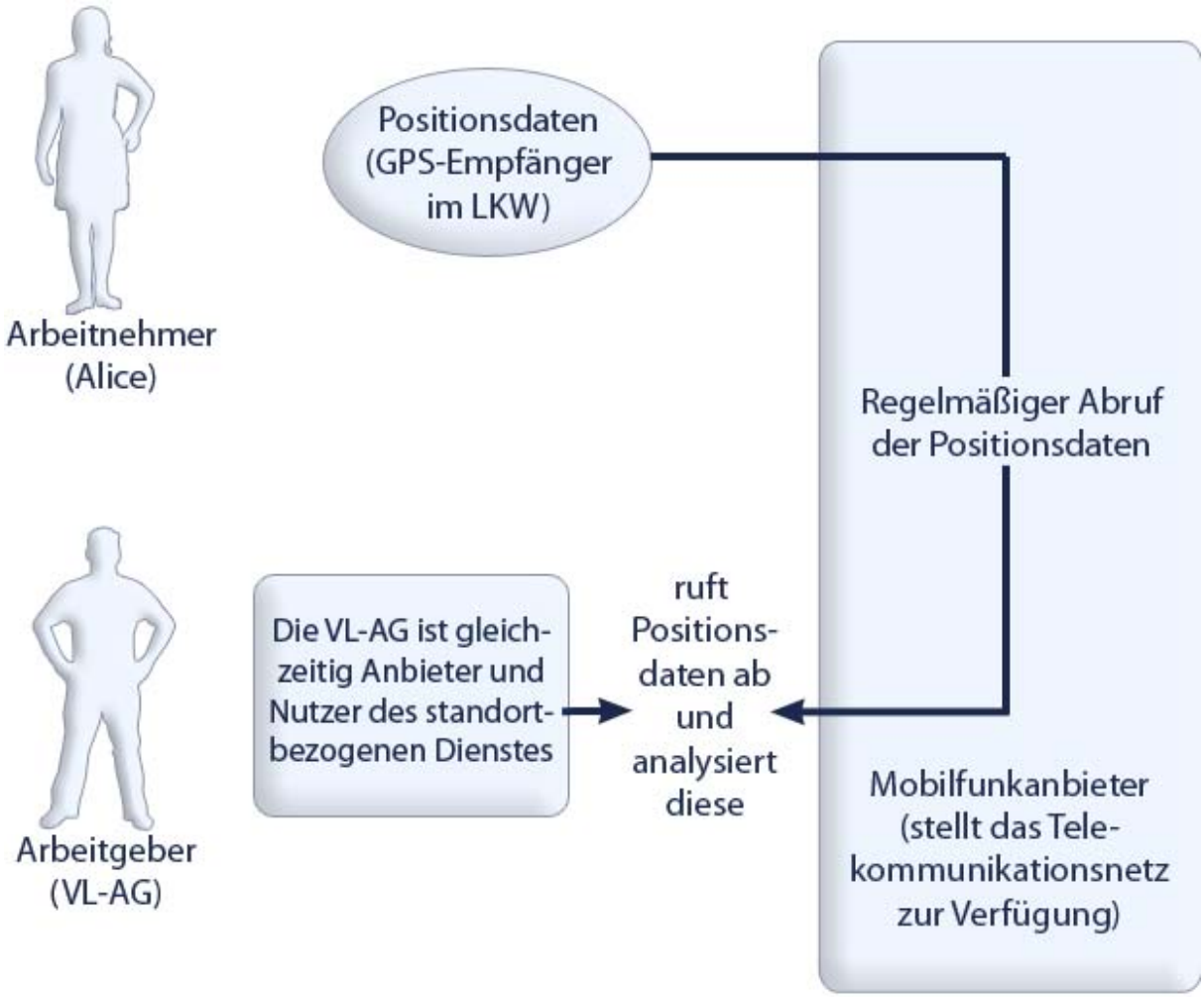


Abbildung 17: Workflow des vorgestellten Tracking-Dienstes

In diesem Szenario sind also mit Alice, der VL-AG und dem Mobilfunkanbieter drei verschiedene Beteiligte zu unterscheiden. Diese sind konkret wie folgt involviert:

- Bei Alice (bzw. dem LKW) handelt es sich um das lokalisierte Subjekt (bzw. Objekt),
- die VL-AG ist gleichzeitig Anbieter und Nutzer des standortbezogenen Dienstes, und
- der Mobilfunkanbieter stellt das Telekommunikationsnetz zur Verfügung.

Die Position des LKW wird mittels eines in das Fahrzeug integrierten Mobiltelefons mit eingebautem GPS-Empfänger ermittelt; es handelt sich hier also um ein terminalbasiertes Ortungsverfahren. Die Positionsdaten werden folglich ausschließlich von der VL-AG generiert, gespeichert und analysiert – der Mobilfunkanbieter ist hingegen nicht an der Lokalisierung beteiligt. Die über die Positionsdaten hinausgehenden Informationen, die für die Erbringung des Dienstes notwendig sind, werden ebenfalls ausschließlich von der VL-AG zur Verfügung gestellt. Es werden also keinerlei Zusatzinformationen von einem externen Content-Provider zugekauft. Der konkrete Dienst ist im Übrigen aus der Perspektive des Nutzers – also der VL-AG – als „Pull"-Service ausgestaltet, da zur Initialisierung des Services ein Kontakt zwischen dem zentralen Server der VL-AG und dem im LKW befindlichen Mobiltelefon hergestellt werden muss.

5.4.3 Verkettung von Daten durch den LBS-Anbieter

Ein standortbezogener Dienst setzt in jedem Fall voraus, dass Standortdaten erhoben und verarbeitet werden. Im Übrigen ist es von der konkreten Ausgestaltung des jeweiligen Dienstes abhängig, welche Daten der LBS-Anbieter im Einzelnen erhebt und miteinander verkettet.

Unterscheiden lassen sich Daten über den Nutzer und solche, die erst nach ihrer Verkettung mit den Nutzerdaten einen Bezug zu diesem aufweisen (z.B. Informationen aus Branchenbüchern oder zur Verkehrslage). Orientiert man sich an der Terminologie des hier grundsätzlich einschlägigen Telemediengesetzes, so ist bei den Nutzerdaten zwischen den folgenden Kategorien zu differenzieren:

- Bestandsdaten,
- Nutzungsdaten und
- Abrechnungsdaten.

Innerhalb der Bestandsdaten wird dabei zwischen Kontaktdaten (wie Name, Anschrift oder Kundennummer) und Profildaten (z.B. Vorlieben oder Hobbys) des Nutzers unterschieden. Werden sie zur Diensterbringung verwendet, so sind die Profildaten gleichzeitig auch Nutzungsdaten. Bei den Standortdaten handelt es sich ebenfalls um Nutzungsdaten. Zu den Abrechnungsdaten gehören schließlich insbesondere Informationen zur Bankverbindung (Name des Kontoinhabers, Kontonummer und Bankleitzahl).

Mit Hilfe der Angaben des Nutzers zu seinen Hobbys oder Interessen sowie der von ihm bei einer Inanspruchnahme des jeweiligen ortsbezogenen Dienstes konkret nachgefragten Informationen (etwa zu Sehenswürdigkeiten oder Restaurants) können Profile über den Nutzer erstellt werden. Außerdem lassen sich umfangreiche Bewegungsprofile erstellen, wenn die Standortdaten in regelmäßigen Abständen und über einen längeren Zeitraum hinweg erfasst, miteinander verkettet und ausgewertet werden.

Dies gilt auch im Falle des oben skizzierten Szenarios, in dem die Standortdaten in regelmäßigen Abständen vom Server der VL-AG bei dem im Fahrzeug befindlichen GPS-Mobiltelefon abgefragt werden und dann miteinander verkettet werden können. Entsprechende Bewegungsprofile können Alice als Fahrerin des LKW zugeordnet und dazu verwendet werden, sie in ihrer Funktion als LKW-Fahrerin zu überwachen.

5.4.4 Rechtliche Implikationen

5.4.4.1 Erstellung von Bewegungsprofilen

Die Erstellung solcher Bewegungsprofile gehört aus der Perspektive des Datenschutzes zu den größten Risiken, die eine Verarbeitung personenbezogener Standortdaten mit sich bringt. Je umfassender und feingranularer solche Bewegungsprofile ausfallen, umso größere Auswirkungen können sie auf das Grundrecht auf informationelle Selbstbestimmung der hiervon betroffenen Person haben. Aus technischer Sicht ermöglicht eine Verkettung von Standortdaten zu Bewegungsprofilen eine umfassende räumliche und zeitliche Überwachung. Darüber hinaus lassen sich aus Bewegungsprofilen u.U. Rückschlüsse auf Beziehungen und Gewohnheiten der getrackten Person ziehen. Auch liefert eine Auswertung solcher Profile in vielen Fällen Aussagen über das zukünftige Verhalten der Betroffenen.

An dieser Stelle sei darauf hingewiesen, dass umfangreiche Datenbestände, die von privaten Stellen vorgehalten werden, stets auch für die Strafverfolgungsbehörden von Interesse sind. Dies gilt auch für die Erhebung und Speicherung von Standortdaten. Als aktuelles Beispiel ist die LKW-Maut zu nennen: Hier sollten die Mautdaten ursprünglich nur für die im Autobahnmautgesetz (ABMG) angegebenen Zwecke – also zu Abrechnungs- und Kontrollzwecken – verwendet werden.[514] Schon bald nach Erlass

[514] §§ 4 Abs. 2, 7 Abs. 2 ABMG.

dieses Gesetzes wurden aber Stimmen laut, die forderten, Mautdaten auch zu Strafverfolgungszwecken zu nutzen. Auch wenn bisher noch keine dies legitimierenden Rechtsgrundlagen geschaffen worden sind, spricht gegenwärtig vieles dafür, dass solche Regelungen in naher Zukunft erlassen werden.[515]

5.4.4.2 Rechtliche Einordnung einer Verwendung von Standortdaten

Standortbezogene Dienste sind in aller Regel als Telemediendienste zu qualifizieren, weshalb die datenschutzrechtliche Zulässigkeit der Verarbeitung personenbezogener Daten durch LBS-Anbieter an den Vorschriften des Telemediengesetzes zu messen ist.[516] Werden solche Dienste mittels netzbasierter Lokalisierungsverfahren realisiert, so werden die Standortdaten auch durch den Telekommunikationsanbieter verarbeitet. Insoweit richtet sich die datenschutzrechtliche Zulässigkeit der Verarbeitung dann nach den Bestimmungen des Telekommunikationsgesetzes.[517]

Nach dessen § 98 darf der Telekommunikationsanbieter die Standortdaten nur anonym oder mit der Einwilligung des Betroffenen zur Bereitstellung von Diensten mit Zusatznutzen verwenden. Zu diesen Diensten gehören auch Location Based Services. Der Telekommunikationsanbieter darf also personenbezogene Standortdaten nur dann an den LBS-Anbieter übermitteln, wenn der jeweilige Nutzer zuvor eingewilligt hat. Der Anbieter des ortsbezogenen Dienstes hingegen darf die Standortdaten nach § 15 Abs. 1 des Telemediengesetzes verarbeiten, soweit sie für die Inanspruchnahme des standortbezogenen Dienstes erforderlich sind. Hier ist eine rechtmäßige Verwendung der Standortdaten also auch ohne eine Einwilligung des Nutzers möglich, weil nur so der jeweilige Vertragszweck erreicht werden kann.

5.4.4.3 Rechtlicher Problemaufriss des skizzierten Szenarios

Die Besonderheit des skizzierten Szenarios besteht darin, dass die Standortdaten des LKW im Rahmen des Arbeitsverhältnisses zwischen der Verkettungs-Logistik AG und Alice verarbeitet werden. Grundsätzlich darf der Arbeitgeber im Rahmen seines Direktionsrechts[518] die Einzelheiten der vom Arbeitnehmer laut Arbeitsvertrag zu erbringenden Leistungen mittels einseitiger Weisungen näher bestimmen. Diese Weisungsbefugnis umfasst Ort, Zeit, Inhalt sowie Art und Weise der vom Arbeitnehmer zu erbringenden Leistung und erstreckt sich damit auch auf die Nutzung standortbezogener Dienste im Unternehmen.

Allerdings wird das Direktionsrecht des Arbeitgebers durch verschiedene rechtliche Vorschriften begrenzt. So ist bei einer Nutzung von standortbezogenen Diensten in Unternehmen zu beachten, dass die Implementierung dieser Dienste sowohl betriebsverfassungsrechtlichen als auch datenschutzrechtlichen Anforderungen genügen muss.[519] Hierbei ist danach zu differenzieren, ob in dem jeweiligen Unternehmen ein Betriebsrat besteht.

Ist dies der Fall, so ist die Implementierung eines standortbezogenen Dienstes nur dann rechtlich zulässig, wenn sowohl ein datenschutzrechtlicher Erlaubnistatbestand als auch eine Betriebsvereinbarung vorliegen.[520] Dabei ist zu beachten, dass eine wirksame Betriebsvereinbarung, die die Modalitäten der Datenverarbeitung regelt, gleichzeitig auch einen datenschutzrechtlichen Erlaubnistatbestand darstellt.

---

[515] Hierzu vgl. etwa http://www.heise.de/newsticker/meldung/87714/ (letzter Zugriff im Oktober 2007).

[516] Schon an dieser Stelle sei darauf hingewiesen, dass das TMG aber dann nicht anwendbar ist, wenn Telemedien im Arbeitsverhältnis zu ausschließlich beruflichen Zwecken bereitgestellt werden. In solchen Fällen, denen auch das soeben skizzierte Szenario zuzuordnen ist, finden dann die allgemeinen Regelungen des Bundesdatenschutzgesetzes Anwendung.

[517] Zur rechtlichen Einordnung einer Verwendung von Standortdaten für Location Based Services vgl. [Jandt 2007].

[518] Dieses wird aus § 315 BGB i.V.m. § 106 GewO abgeleitet.

[519] Ausführliche Ausführungen hierzu finden sich bei [Hallaschka/Jandt 2006].

[520] Eine Betriebsvereinbarung ist deshalb erforderlich, weil die Implementierung eines standortbezogenen Dienstes in einem Unternehmen gem. § 87 Abs. 1 Nr. 1 und 6 BetrVG mitbestimmungspflichtig ist.

Besteht in dem jeweiligen Unternehmen hingegen kein Betriebsrat oder kommt – trotz Bestehens eines Betriebsrats – keine Betriebsvereinbarung zustande, so ist die Datenverarbeitung an den Vorschriften des Bundesdatenschutzgesetzes zu messen. Dies resultiert daraus, dass es bislang keine bereichsspezifischen Regelungen zum Arbeitnehmerdatenschutz gibt und dass die datenschutzrechtlichen Vorschriften des Telemediengesetzes, die bei einem Einsatz von standortbezogenen Diensten grundsätzlich zu beachten sind, nach § 11 Abs. 1 Nr. 1 TMG dann nicht anwendbar sind, wenn Location Based Services im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken bereitgestellt werden. Als datenschutzrechtliche Erlaubnistatbestände kommen deshalb in solchen Konstellationen § 28 Abs. 1 Nr. 1 BDSG, der eine Verarbeitung standortbezogener Daten im Unternehmen dann gestattet, wenn diese für die Durchführung des Arbeitsvertrags erforderlich ist, oder eine wirksame[521] Einwilligung des Arbeitnehmers in Betracht.

5.4.5 Fazit

Standortbezogene Dienste gewinnen mehr und mehr an Bedeutung und bieten den Nutzern in vielen Fällen einen Mehrwert. Jedoch können die hierbei anfallenden Daten auch dazu verwendet werden, – missbräuchlich – Bewegungs- und Interessensprofile der Nutzer zu erstellen.

Werden standortbezogene Dienste in Unternehmen eingesetzt, so kann der Arbeitgeber die Standortdaten dazu verwenden, seine Arbeitnehmer bei ihrer beruflichen Tätigkeit zu überwachen. Aus rechtlicher Sicht setzt die Verwendung von standortbezogenen Diensten in Unternehmen stets das Vorliegen eines datenschutzrechtlichen Erlaubnistatbestands voraus. Existiert in dem jeweiligen Unternehmen eine Arbeitnehmervertretung, so ist darüber hinaus zu berücksichtigen, dass die Einführung von Location Based Services der Mitbestimmungspflicht des Betriebsrats unterliegt.

5.5 Szenario 4: Ubiquitous Computing – Ambient Assisted Living

5.5.1 Allgemeines

In unserem Alltag nutzen wir bereits heute eine Vielzahl von „intelligenten“ Gegenständen, die entwickelt wurden und werden, um unseren Tagesablauf zu erleichtern. Diese elektronischen Helfer, wie beispielsweise Mobiltelefone, Chips in Kreditkarten, Navigationssysteme, lichtabhängige Steuerungssysteme für die Innenbeleuchtung oder Rollläden von Häusern oder intelligente Wärmeregelungssysteme in Gebäuden, erfüllen ihren Zweck mittels Kommunikationstechnik und Informationstechnologie. Durch Fortschritte in den technischen Entwicklungen dieser Bereiche nimmt die Miniaturisierung dieser elektronischen Helfer fortwährend zu. Es gibt sowohl immer kleinere Sensoren, die passiv verschiedenste Umgebungsinformationen erfassen, als auch immer energieeffizientere und günstigere Prozessoren, die aktiv mit ihrer Umgebung kommunizieren und diese untersuchen können. Es erscheint nicht länger visionär, für die Zukunft eine von Informationstechnologie durchdrungene Welt zu erwarten. Dabei sind neben sozialen Fragen wie Akzeptanz auch rechtliche Fragen zu beantworten. Die Steuerungsmöglichkeiten von intelligenten Systemen für den Einzelnen, Transparenzfragen und Einwilligung in die Datenverarbeitung sind dabei mit der Vernetzung und Miniaturisierung einhergehende Fragestellungen.

5.5.2 Ambient Intelligence und Ambient Assisted Living

Ambient Intelligence (AmI) und deren Teilaspekt *Ambient Assisted Living* (Assistiertes Leben) steht für eine intelligente Umgebung, die sensitiv und adaptiv auf die Anwesenheit von Menschen und Objekten reagiert. Der Begriff wird oft synonym eingesetzt für *Ubiquitous Computing*[522] und *Pervasive Computing*. Eine Abgrenzung dieser Begriffe unternimmt [TAUCIS 2006]: Ausgehend von der traditionellen Datenverarbeitung mit Servern, PCs, Terminals und traditionellen Ein- und Ausgabe-

[521] Im Verhältnis von Arbeitgeber zu Arbeitnehmer kann insbesondere fraglich sein, ob eine freiwillige Einwilligung vorliegt.

[522] Der Begriff wurde eingeführt von [Weiser 1991].

geräten als Interface führt eine Erhöhung der Mobilität zum *„Mobile Computing“* – eine verstärkte Einbettung miniaturisierter Computer in andere Gegenstände zum „Pervasive Computing“. Von Ubiquitous Computing, also allgegenwärtiger Datenverarbeitung, spricht man, wenn beide Aspekte zusammen kommen.[523]

Der Begriff Ambient Intelligence[524] beschreibt im Wesentlichen Ubiquitous Computing. Dabei wird angenommen, dass problematische Bereiche der Einführung gelöst sind (soziale Akzeptanz, detaillierte Verhaltensprofile, Abrechnung von Dienstleitungen etc.).

Es werden zahlreiche Einsatzbereiche von AmI unterschieden, abhängig von der Lebenssituation, in der das jeweilige System zum Einsatz kommt. Eine nicht abschließende Übersicht gibt Tabelle 17:[525]

Einsatzbereich	**Lebenssituation**
Ambient Assisted Living	allein lebender, älterer Mensch
Ambient Assisted Working	arbeitender Mensch
Ambient Assisted Education	Wissen aufnehmender Mensch
Ambient Assisted Transportation	Fortbewegung des Menschen
Ambient Assisted Leasure	Mensch in der Freizeit

Tabelle 17: Einsatzbereiche von Ambient Intelligence

Ambient Assisted Living (AAL – assistiertes Leben) sucht nach technischen Mitteln, um älteren Menschen möglichst lange ein selbstbestimmtes Leben in ihrer gewohnten Umgebung (sprich Haus oder Wohnung) zu ermöglichen. Durch geeignete, unauffällige, unsichtbare und leicht bedienbare Elektronik sollen sie dabei unterstützt werden. Ziele sind dabei insbesondere, ihnen den Tagesablauf zu erleichtern (Komfort), die Wohnung sicherer zu machen (Sicherheit) und bei gesundheitlichen Problemen und in Notsituationen helfen zu können (Gesundheit).

Je nach Einsatzbereich werden dazu Vital- und Bewegungsdaten des Menschen (Gesundheit) oder die Umgebung und benutzte Technik (Sicherheit und Komfort) überwacht.[526] So sollen Notfall-situationen erkannt und eine Alarmierung in Abhängigkeit der erkannten Schwere der Notsituation erfolgen

Eine Übersicht[527] verfügbarer oder in Entwicklung befindlicher Systeme des assistierten Lebens gibt Tabelle 18:

[523] Vgl. auch [Mattern 2007].

[524] Geprägt wurde der Begriff durch die Information Society Technologies Advisory Group der EU. ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-99-final.pdf (letzter Zugriff im Oktober 2007).

[525] Angelehnt an ISTAG „Scenarios for Ambient Intelligence in 2010“, 2001. Verfügbar unter ftp://ftp.cordis.europa.eu/pub/ist/docs/istagscenarios2010.pdf (letzter Zugriff im Oktober 2007).

[526] Szenarien finden sich beispielsweise bei: Safeguards in a World of Ambient Intelligence (SWAMI – http://ec.europa.eu/research/fp6/ssp/swami_en.htm (letzter Zugriff im Oktober 2007)), Deliverable 1 und 2. Verfügbar unter http://swami.jrc.es/pages/ (letzter Zugriff im Oktober 2007). Weiterhin: ISTAG „Scenarios for Ambient Intelligence in 2010“ und AAL „Europe is facing a demographic challenge – Ambient Assisted Living offers solutions“.

[527] Ausführlich zu Ambient Assisted Living in Deutschland: VDI/VDE-IT „AAL – Country Report Germany“, abrufbar unter http://www.aal169.org/Published/CRgermany.pdf (letzter Zugriff im Oktober 2007).

Einsatz zur Verbesserung von ...	Funktionalität
... Gesundheit	● Sturzerkennung ● Medikamenteneinnahme ● Notfallsituationen erkennen ● Notrufarmbänder
... Sicherheit	● Türüberwachung, Haustürkamera ● Abschalten elektrischer Verbrauch, z.B. bei Verlassen der Wohnung ● Wasserschaden: Alarm
... Komfort	● elektronischer Schlüssel ● fernsteuerbare Rollläden ● automatische Lichtfunktion ● Telefonieren über Bildaufruf

Tabelle 18: Überblick über verschiedene Systeme des Ambient Assisted Living

Nachstehendes Szenario stellt Einsatzmöglichkeiten von Ambient-Assisted-Living-Systemen im Bereich Gesundheit dar[528].

5.5.3 Szenario: Notfallsituationen erkennen

Alice und Bob haben in den letzten Jahren manchmal Schwierigkeiten damit, Dinge, die ihnen früher leicht fielen, heute genauso leicht und schnell zu erledigen. Bob ist aufgrund seines Gesundheitszustands in seiner Mobilität eingeschränkt. Meist ist er gezwungen, den ganzen Tag im Bett zu liegen und kommt dann aus eigener Kraft nicht aus dem Bett. Auch Alice muss für längere Wege einen Rollator benutzen. So beweglich wie noch vor einigen Jahren fühlen sich die beiden nicht mehr. Beiden ist es bereits passiert, dass sie in ihrer Wohnung ins Straucheln geraten sind und beinahe gestürzt wären. Dazu kommt, dass Alice Probleme mit ihrem Blutdruck hat. Bislang hat sie schon drei Mal das Bewusstsein verloren. Glücklicherweise immer nur dann, wenn sie nach dem ersten Schwindelgefühl schon sicher auf dem Sofa saß. Ihr Sohn, der als Arzt im örtlichen Krankenhaus arbeitet, hat sie aus Sorge ermahnt, ein Bruch könne in ihrem Alter schwerwiegende Folgen haben. Er hat Alice und Bob geraten, ihre Wohnung mit einem Notfallsystem auszustatten. Denn im Falle eines Sturzes, das weiß er durch seine Arbeit, zählt jede Minute, um die Chance auf Heilung zu erhöhen. Hantiert Alice gerade mit dem Bügeleisen oder am Herd, kann außerdem auch ein Wohnungsbrand Folge ihrer Bewusstlosigkeit sein. Und was wäre, wenn Alice einmal ausgerechnet dann das Bewusstsein verliert, wenn Bob nicht aus dem Bett aufstehen kann?

Das System, für das die beiden sich entschieden haben, heißt „Safe Home“ und besteht aus zwei sich ergänzenden Technologien. In Fußmatten auf dem Boden sind Sturzsensoren eingebaut. Diese registrieren die Erschütterung, die bei einem Sturz auftritt. Ein Lesegerät liest über Funk in kurzen Abständen die von den Sensoren gemessenen Werte aus. Wird dabei ein festgelegter Schwellenwert überschritten, löst dies einen Alarm aus. Das System informiert selbstständig die Notfallzentrale des Anbieters. Durch die übermittelte Kennung wissen die Mitarbeiter sofort, bei welchem Kunden der Alarm ausgelöst wurde. Alice und Bob haben mit dem Anbieter einen abgestuften Alarmierungsplan

[528] R. Orr und G. Abowd „The Smart Floor: A Mechanism for Natural User Identification and Tracking“, abrufbar unter ftp://ftp.cc.gatech.edu/pub/gvu/tr/2000/00-02.pdf (letzter Zugriff im Oktober 2007). S. Dalal et al. „A Rule-Based Approach to the Analysis of Elder's Activity Data: Detection of Health and Possible Emergency Conditions“, abrufbar unter http://marc.med.virginia.edu/pdfs/library/FS205DalalS.pdf (letzter Zugriff im Oktober 2007). T. Barger et al. „Health Status Monitoring Through Analysis of Behavioral Patterns“, abrufbar unter http://marc.med.virginia.edu/pdfs/library/ambient%20intelligence.pdf (letzter Zugriff im Oktober 2007). M. Alwan et al. „A Smart and Passive Floor-Vibration Based Fall Detector for Elderly“ abrufbar unter http://marc.med.virginia.edu/pdfs/library/ICTTA_fall.pdf (letzter Zugriff im Oktober 2007).

vereinbart. Bevor dieser einen Krankenwagen ruft, wird zwei Minuten lang versucht, Alice oder Bob telefonisch zu erreichen. Der Anbieter bestätigt zudem, dass das System nicht zwischen dem Sturz eines Menschen und einem schweren, fallen gelassenen Gegenstand unterscheiden kann.

Wenn Alice das Bewusstsein verliert, muss es allerdings nicht zwangsläufig auch zu einem Sturz kommen. Trotzdem wird sie auch in diesen Fällen vielfach dringend auf eine ärztliche Versorgung angewiesen sein. Deshalb wollen Alice und Bob ihr Notfallsystem um eine Bewegungsfunktion erweitern lassen. Dabei nehmen vier in der Wohnung verteilte Kameras Bewegungen auf. Das System ist intelligent und kann, wenn man es installiert, die Bewegungsmuster und Tagesabläufe der Bewohner lernen. Auffällige Bewegungen, die auf ein gesundheitliches Problem hindeuten oder Situationen, in denen sich die Bewohner gar nicht mehr bewegen, erkennt das System selbstständig. Es ist noch nicht gelungen, Schlaf von Bewusstlosigkeit zu unterscheiden. Daher ist auch für diese Funktion eine Abstufung eingeplant. Bevor bei Bewegungslosigkeit ein Alarm ausgelöst wird, sendet die Anlage ein akustisches Signal. Alice und Bob haben dann zwei Minuten Zeit, die Alarmierung der Zentrale zu verhindern. Dazu können sie entweder einen Knopf am Schaltkasten des „Safe Home“ Systems oder aber einen Knopf an dem zusätzlichen Notrufarmband, das beide tragen, betätigen. Gleichzeitig mit der Zentrale von „Safe Home“ erhält auch ihr Sohn eine Notrufmeldung auf sein Mobiltelefon.

Am Anfang hatte Bob Bedenken wegen der Kameras. Er wollte sich in seiner eigenen Wohnung nicht beobachtet fühlen. Aber seine Bedenken haben sich zerstreut, nachdem er sich das System genau hat erklären lassen und sich sodann für folgende Lösung entschieden hat: Die Kamerabilder werden nicht an den Anbieter übermittelt und auch nicht aufgezeichnet. Stattdessen findet eine Echtzeitauswertung statt, um auffälliges Verhalten zu erkennen, das von den erlernten Gewohnheiten der Bewohner abweicht. Wie das genau funktioniert, wissen Bob und Alice zwar nicht. Aber sie sind zufrieden, weil sie selbst im Falle eines Alarms eingreifen können, falls das System etwas falsch bewertet hat. Auch wenn „Safe Home“ keinen Sturz verhindern wird, sind sie jedenfalls sicher, schnell Hilfe zu erhalten, falls doch einmal etwas passiert. Der Anbieter bietet das System auch in einer zweiten Konfiguration an: Wenn dabei nicht innerhalb von zwei Minuten die Alarmübermittlung verhindert wird, werden die von den Kameras erfassten Bilder an die Zentrale übertragen, damit die Mitarbeiter sehen können, ob ein Notfall vorliegt. Damit soll eine Fehlalarmierung von Sicherheitskräften verhindert werden. Wohl bei der Vorstellung, dass unvermittelt Fremde einen Blick in ihr Wohnzimmer werfen können, war es Alice und Bob aber nicht, weshalb sie sich dagegen entschieden.

5.5.4 Verkettung von Daten durch den Serviceanbieter

Im Rahmen von AmI-Anwendungen ist es technisch immer häufiger möglich, Gegenstände in einem Speicher zurückliegende Aktivitäten protokollieren zu lassen und sie so mit einem „Gedächtnis“ auszustatten.

Die im Rahmen von Ambient-Intelligence-Systemen verarbeiteten Daten können dabei aufgrund der Durchdringung von immer mehr Lebensbereichen vielfältige Datenkategorien umfassen. Je nach Anwendung werden beispielsweise Standortdaten, Bestandsdaten, Nutzungsdaten und Abrechnungsdaten (zum Beispiel im Transportbereich) oder auch Inhaltsdaten (wie z.B. sensible medizinische Daten) erfasst und miteinander verkettet.

Ambient Intelligence schafft im Hinblick auf Datenschutz und informationelle Selbstbestimmung neue Probleme. Intelligente Gegenstände und eine mit Sensoren versehene Umwelt führen Datenverarbeitungsschritte im Hintergrund aus, um dem Benutzer Dienste ohne großen Aufwand für diesen jederzeit anbieten zu können. Dabei sind die Systeme gezielt so gestaltet, dass sie im Hintergrund arbeiten und keine Aufmerksamkeit des Benutzers erfordern, auch wenn je nach System Steuerungsmöglichkeiten für den Nutzer bestehen. In vielen Fällen wird dieser zum Zwecke der Authentisierung von Sensoren erfasst und identifiziert[529]. Das Zusammenführen von im Hintergrund erfassten Erkenntnissen ist technisch grundsätzlich möglich, indem Personen über charakteristische (zum Beispiel biometrische) Merkmale oder spezielle im System eingesetzte Identifikatoren identifiziert werden. Über Identifikatoren oder durch von intelligenten Gegenständen erkanntes

[529] Ein Beispiel für die Unterscheidung von Personen anhand ihrer Art, sich zu bewegen, findet sich bei http://www.cs.cmu.edu/~nursebot/web/tracking/floor3Drle.gif (letzter Zugriff im Oktober 2007).

wiederkehrendes Verhalten lassen sich Informationen über Personen verketten. Das Ambient-Intelligence-System verknüpft dazu die von Sensoren erfassten Daten mit weiteren internen und externen Daten. Eine darauf basierende adaptive Entscheidungsfindung steuert den zu erbringenden Dienst und löst Aktionen aus. Dabei findet eine Personenerkennung und Verhaltensanalyse statt.

5.5.5 Rechtliche Implikationen

AmI-Anwendungen betreffen aufgrund ihrer soeben geschilderten Struktur zumeist das Recht auf informationelle Selbstbestimmung. Dabei verstärkt die allgegenwärtige Datenverarbeitung bereits bestehende Rechtsprobleme. Die intelligente Umgebung geht einher mit funktionalen datenschutzrechtlichen Risiken. Stattfindende Datenflüsse und Datenverarbeitungsschritte sind für den Betroffenen aufgrund der Miniaturisierung der Systeme schwer nachvollziehbar. Nicht immer geht der Einsatz von intelligenten Gegenständen daher einher mit einer bewussten Aufgabe von Privatheit durch die selbstbestimmte Entscheidung für den Einsatz eines AmI-Systems und damit vielfach auch die Möglichkeit einer intelligenten Überwachung. Insoweit besteht also ein technikbedingter Kontrollverlust. Durch systemimmanente Intransparenz hinsichtlich der stattfindenden Datenverarbeitung und der datenschutzrechtlichen Verantwortung (Daten verarbeitende Stelle) erschwert allgegenwärtige (verteilte) Datenverarbeitung die Geltendmachung von Betroffenenrechten.

Auch für die im Rahmen von Ambient Intelligence stattfindende Verarbeitung von personenbezogenen Daten gelten die grundsätzlichen datenschutzrechtlichen Anforderungen. Je nachdem, welche Art von Daten verarbeitet wird, können zudem bereichsspezifische Rechtsgrundlagen einschlägig sein. Eine Einwilligung des Betroffenen oder eine rechtliche Erlaubnis für die Datenverarbeitung ist erforderlich.

In dem vorliegenden Szenario ist die Datenverarbeitung nach § 28 Abs. 1 Nr. 1 BDSG gestattet. Zwischen dem Betreiber von „Safe Home“ und Alice und Bob besteht ein Vertrag über das Erbringen der Leistung „Notfallsystem“. Vertragsgegenstand ist die automatische Erkennung von Notfallsituationen und jedenfalls an der Art und Weise der Überwachung durch das System besteht für Alice und Bob kein Transparenzdefizit. Sie haben sich dabei für die grundsätzlich weniger invasive Nutzungsvariante entschieden, die keine Übertragung von Kamerabildern an Mitarbeiter der „Safe Home“-Notfallzentrale vorsieht.

Grundsätzlich gilt, dass für eine durch vernetzte und allgegenwärtige Datenverarbeitung technisch mögliche unbemerkte Erfassung von Personen und ihnen zugeordneten Objekten oder Verhaltensweisen sowie einer damit einhergehenden Profilbildung eine Einwilligung des Betroffenen erforderlich ist. Eine solche Datenverarbeitung lässt sich in aller Regel weder durch § 28 Abs. 1 Nr. 1 BDSG stützen (weil kein Vertrag besteht) noch durch § 28 Abs.1 Nr. 2 BDSG (weil das schutzwürdige Interesse des Betroffenen bei einer heimlichen Überwachung und Auswertung seines Verhaltens das Interesse der Daten verarbeitenden Stelle überwiegt) legitimieren.

Wichtige Aspekte[530] bei der Bereitstellung von Ambient-Intelligence-Systemen sind das Schaffen von Vertrauen durch Transparenz[531] und Kontrollmöglichkeiten, die Frage der Zurechenbarkeit[532] von ausgelösten Aktionen, eine datensparsame Technikgestaltung sowie technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung.

5.5.6 Fazit

Das vorstehende Szenario beschreibt einen positiven, weil gewünschten Einsatz[533] von Ambient Assisted Living. Dies soll nicht darüber hinweg täuschen, dass auch bei vermeintlich hehren Zielen oder positiven Zwecken des Einsatzes von AmI-Systemen die systemimmanenten Probleme wie

[530] Dazu: [TAUCIS 2006].

[531] Diese ist bereits Voraussetzung für eine informierte Einwilligung und auch eine rechtliche Zulässigkeit der Datenverarbeitung gestützt auf § 28 Abs. 1 BDSG.

[532] Siehe [Mattern 2007].

[533] Negative Szenarien des AmI beschreibt SWAMI „Dark Scenarios in Ambient Intelligence: Highlighting Risks and Vulnerabilities“, abrufbar unter http://swami.jrc.es/docs/SWAMI_D2_scenarios_Final.pdf (letzter Zugriff im Oktober 2007).

Intransparenz und verteilte Datenverarbeitung die Ausübung des Rechts auf informationelle Selbstbestimmung zumeist erschweren. Gleiches gilt für die Ausübung der Betroffenenrechte. Die zukünftige technische Entwicklung muss deshalb beobachtet und der bestehende Rechtsrahmen darauf hin überprüft werden, ob durch ergänzende Rechtssetzung korrigierend eingegriffen werden muss.[534]

[534] BVerfGE 112, 304 = MMR 2005, S. 371. Hierzu auch [Roßnagel 2007, S. 199 ff.].

6 Ergebnisse und Handlungsempfehlungen

6.1 Ergebnisse

Verkettung von Identitätsdaten ist ein inhärenter Bestandteil des persönlichen Lebens. Dies gilt für jede Privatperson schon in ihrer Entwicklung vom Kind zum Erwachsenen und ist dabei Bestandteil eines lebenslangen Lernprozesses. Auch Gesellschaft basiert auf Verkettung – Vertrauen und Erwartungssicherheit beruhen zum großen Teil auf Erkenntnissen, die durch Verkettung gewonnen wurden.

Wie diese Arbeit gezeigt hat, sind Organisationen Verkettungsmaschinen, d.h., sie betreiben professionell Informationsanreicherung für ihre jeweiligen Zwecke. Dies gilt gleichermaßen für staatliche Behörden als auch privatwirtschaftliche Unternehmen – und auch für Communities im Web 2.0 –, wobei jedoch einige Unterschiede hervorzuheben sind:

- Der **Staat** sammelt gesetzlich festgelegt Daten über Individuen, von denen einige sogar von der Geburt bis über den Tod hinaus gespeichert bleiben. In Fällen der staatlichen Planung reichen statistische Daten aus. Für die Ausübung des Gewaltmonopols kann eine Verkettung zur Person in bestimmten Fällen sogar den Zugriff auf den Körper des Betroffenen umfassen, z.B. wenn der Betroffene geschützt werden muss oder wenn andere vor dem Betroffenen zu schützen sind. Daten über psychologische Profile von rechtstreuen Bürgern werden in der Regel nicht von staatlichen Stellen gesammelt und verkettet. Bei der Strafverfolgung oder Gefahrenabwehr kann dies aber anders sein: Dann werden u.U. alle Daten, die irgendwie verfügbar sind, zur Lösung eines Falls oder zum Zugriff auf einen Täter (oder Zeugen) verkettet. Investigative Tendenzen, bei denen auch intimere Details der Persönlichkeit eingehen können, kann man außerdem dort feststellen, wo es um die Verhinderung von Leistungsmissbrauch geht. Dies geschieht heute allerdings noch nicht primär im Bereich der digitalen Welt. Außerdem wird durch die Einführung von Vorratsdatenspeicherung eine Grundlage für eine einfachere Auswertbarkeit von Daten auch unbescholtener Bürger gelegt.
- Der Erfolg eines **Unternehmens** hängt zumeist davon ab, inwieweit es der Firma gelingt, (potenzielle) Kunden für ihre Produkte zu interessieren und an sich zu binden. In diesem Bereich besteht ein Markt für alle möglichen Akteure in Bezug auf Informationsbereitstellung und -anreicherung, vom Adresshändler bis zum Scoring-Unternehmen. Für die eigentlichen Transaktionen wären darüber hinausgehende Daten gar nicht erforderlich, aber Kundenbindungssysteme und Konzepte zum immer gezielteren Marketing sammeln und verketten alle Daten, die dem Zweck dienlich scheinen. Dies umfasst insbesondere Daten zu psychologischen und zu Interessensprofilen, um eine darauf zugeschnittene Produktwerbung zielgenau bei dafür empfänglichen Personen zu platzieren. Es ist noch unklar, ob es sich aus Unternehmenssicht auch lohnt, lang zurückreichende Daten zu sammeln und auszuwerten, oder ob es reicht, mit recht aktuellen Daten über Kunden zu arbeiten. Ein Zugriff auf den Körper der Betroffenen ist in den wenigsten Fällen nötig; jedoch gibt es Geschäftsmodelle, die auf eine Bindung an eine Person setzen und dabei beispielsweise eine Authentisierung mit biometrischen Merkmalen erforderlich machen.
- In **Communities** geben Menschen alle möglichen Daten von sich (und auch über andere) frei und nehmen an sozialen Netzwerken teil. Die Verkettung dieser digitalen Identitäten liefert in vielen Fällen sogar mehr Informationen als das, was Staat und Organisationen in Erfahrung bringen. Allerdings ist die Authentizität der Informationen in der Community-Welt nicht garantiert, und einige Mitwirkende nutzen dies aus, indem sie auch falsche Informationen streuen oder sich als andere Leute ausgeben. Die Langfristfolgen für diese massiven Datenfreigaben durch Individuen, die andere global sammeln, verketten auswerten können, sind noch nicht absehbar, auch wenn jetzt schon nicht nur in Einzelfällen die im Internet verfügbaren Daten bei Personaleinstellungen gezielt ausgewertet oder staatliche Einreiseverbote aufgrund von Bücherwunschlisten verhängt werden.

Die technische Entwicklung hat hier in den letzten Jahren massiv Vorschub geleistet, und weitere Fortschritte in Quantität und Qualität bei der Informationsanreicherung sind zu erwarten. Daten über Individuum liegen zunehmend digital vor und sind damit in vielen Fällen leichter zugreifbar, verkettbar und auswertbar. Da nicht nur unmittelbar personenbezogene Daten betroffen sind, sondern auch mit der Verarbeitung anonymer und pseudonymer Daten Auswirkungen auf Einzelne oder Gruppen von Individuen verbunden sein können, geht das Thema über den Bereich des heutigen Datenschutzes hinaus. Internationale Privacy-Ansätze, die auf den Schutz der Privatheit in ihren einzelnen Facetten zielen, können hier die Diskussion befruchten.

Es ist wichtig, dass sich die Akteure im Handlungsfeld, also insbesondere Technikgestalter, aber auch Recht und Politik, dieses Trends zu mehr Verkettung digitaler Identitäten bewusst werden. Um diesen Trend für die Gestaltung und Weiterentwicklung einer funktionierenden, demokratischen Informationsgesellschaft zu lenken, müssen Methoden geschaffen und implementiert werden, um Verkettung unter Bedingungen zu stellen. Die Bedingungen sind dann im gesellschaftlichen Diskurs festzulegen.

6.2 Handlungsempfehlungen

Aus dieser Arbeit ergibt sich eine Vielzahl von Handlungsempfehlungen, die sich an verschiedene Akteure richten: In diesem Abschnitt zeigen wir Empfehlungen auf für

- Technikgestalter,
- Recht und Politik sowie
- Forschungsförderung.

Abgesehen von den unmittelbaren Resultaten dieser Arbeit sind hier auch Ergebnisse aktueller Gutachten und Studien eingeflossen, so z.B. [TAUCIS 2006], [Roßnagel 2007] und [GI-Memorandum 2007].

6.2.1 Handlungsempfehlungen – Gestaltung von Technik und Prozessen

Die Handlungsempfehlungen im Bereich Technik adressieren primär das Gestalten von Informations- und Kommunikationssystemen sowie damit in Zusammenhang stehenden Prozessen, um die Verkettung digitaler Identitäten unter Bedingungen stellen können. Dazu gehören insbesondere Transparenz und Steuerbarkeit für den Betroffenen sowie Maßnahmen zur Qualitätssicherung.

6.2.1.1 Transparenz

Transparenz über die Datenverarbeitung ist generell wichtig, damit Betroffene ihr Recht auf informationelle Selbstbestimmung wahrnehmen können. Im Zusammenhang mit Verkettung sind zu unterscheiden: das Bewusstmachen von Verkettungsmöglichkeiten, Informationen über die eigentliche Aktion der Verkettung sowie das nachträgliche Wissen nach erfolgter Verkettung. Hinzu kommt Transparenz für die Betroffenen über ihre Steuerungsmöglichkeiten und Freiheitsgrade in Bezug auf Verkettung, was im Anschluss (siehe Abschnitt 6.2.1.2) erläutert wird.

6.2.1.1.1 Transparenz über Verkettungsmöglichkeiten

Bereits im Vorfeld von möglichen Verkettungen sollten Menschen das Datensammel- und Verkettungspotenzial erkennen können. Dies beginnt schon bei den technischen Geräten, die eine Überwachung erlauben, wozu grundsätzlich Videokameras, Mobiltelefone, Endgeräte an digitalen Telefonanlagen oder auch RFID-Chips gehören. Um die Transparenz zu gewährleisten, sollten alle Geräte gekennzeichnet werden, z.B. durch genormte Logos oder Icons auf den Geräten oder durch Hinweisschilder in den Räumen, in denen die Geräte zum Einsatz kommen.

Auch über mögliche Verkettungen sollte vorab informiert werden, z.B. indem bereits bei der Vergabe von Adressen und Accounts oder anderen Verkettungsmerkmalen herausgestellt wird, welche Verkettbarkeiten innerhalb der Datenbestände oder mit anderen Daten erkennbar sind. Dies kann sich aus offengelegten Strukturinformationen zu den Daten und Datenbanken ergeben, wodurch zumindest Experten oder Aufsichtsbehörden die Verkettungsmöglichkeiten erschließbar sein sollten.

6.2.1.1.2 Transparenz über Verkettung

Wie bei der Aufzeichnung auf Band und der Videoüberwachung, so sollten auch bei Verkettung von Daten bzw. der Datensammlung die Betroffenen im Vorfeld darüber informiert werden. Daher sollte dem Betroffenen angezeigt werden, wenn ein Gerät gerade aktiv überwacht, z.B. durch eine rote Lampe bei Audio- oder Videoaufzeichnung oder gar durch akustische Signale.

Auch die Überwachungsbereiche, d.h. Räume oder Raumteile, in denen überwacht wird, sollten gekennzeichnet sein. Im Fall von Videokameras könnte dies der von der Kamera abgedeckte Bereich sein, beim Auslesen von RFID-Chips im Supermarkt wäre es beispielsweise der Kassenbereich.

Die Erkennbarkeit von zur Überwachung eingesetzten Geräten sollte nicht nur (audio-)visuell, sondern auch zusätzlich auf technischer Ebene unterstützt werden. Dies umfasst die Entwicklung von Geräten in der Hand des Nutzers, die die Aktivität von Sensoren, Kameras, Mikrofonen oder Lesegeräten erkennen, anzeigen und protokollieren. Es sollte auch unmittelbar über die verantwortliche Stelle informiert werden, damit Betroffene dort ggf. ihre Rechte wahrnehmen können.

Nicht nur für Überwachung, sondern auch in Bezug auf die Verarbeitung der Daten muss jeweils für die Betroffenen klar sein, welche Daten wie verarbeitet werden und wer alles auf die Daten Zugriff hat. Zwar sind „Privacy Policies“ (Datenschutzerklärungen) schon Standard bei Websites, doch deren Inhalte sind in den wenigsten Fällen für Nutzer verständlich. Zumindest sollten sich solche Privacy Policies an Vorgaben orientieren, wie sie von der europäischen Art. 29-Datenschutzgruppe in ihrer „Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten“ [Art. 29-Datenschutzgruppe 2004] formuliert wurden: In einer Mehrebenen-Struktur (engl.: „multi-layered structure“) werden die notwendigen Information im jeweils angemessenen Detaillierungsgrad gegeben, was die Verständlichkeit für den Nutzer erhöht.[535]

Solche Privacy Policies können von Datenschutzmanagement-Systemen unterstützt werden, die die darin enthaltenen Angaben zur Datenverarbeitung, vor allem auch die diesbezüglichen Beschränkungen auf Zwecke, Dauer oder Zugriffsberechtigte, auch tatsächlich umsetzen.

6.2.1.1.3 Transparenz nach einer Verkettung

Auch im Nachhinein sollten Verkettungen den Betroffenen bewusst sein können. Ähnlich dem Einzelverbindungsnachweis der Telekommunikationsunternehmen ließe sich ein Einzelnutzungsnachweis (vgl. [Köhntopp/Pfitzmann 2000]) einführen, der dem Betroffenen detailliert jede Nutzung seiner Daten mitteilt, beispielsweise per E-Mail. Der Betroffene könnte ihn wie einen Kontoauszug sichten und sich bei Unstimmigkeiten an den Verarbeiter wenden. Es bliebe ihm überlassen, ob er seine Einzelnutzungsnachweise bei sich sammelt (z.B. in einem Identitätsmanager in Hand des Nutzers, in dem diese Protokolle gesammelt werden) oder diese löscht. Man könnte überlegen, in ähnlicher Weise auch über geplante Verkettungen zu informieren, wobei der Betroffene dem dann widersprechen könnte oder sogar explizit seine Zustimmung geben müsste.

Darüber hinaus sollten Betroffene stets die Möglichkeit haben, ihr Rechte auf Auskunft, Korrektur und Löschung geltend zu machen, und zwar auch bei pseudonymen Daten. Dies wird u.a. im Telemediengesetz gefordert, doch läuft es häufig leer, weil keine sichere Zuordnung der Daten zum Betroffenen hergestellt werden kann und Betroffene lediglich Auskunft zu ihren eigenen Daten erhalten dürfen. Ein Beispiel dafür sind Cookies, bei denen es sich sehr wohl um personenbezogene Daten handelt, die

[535] Siehe auch das Berliner Memorandum zu Datenschutzerklärungen, S. 91 ff. in LDA Brandenburg/Berliner Beauftragter für Datenschutz und Informationssicherheit: Dokumente zu Datenschutz und Informationsfreiheit 2004, abrufbar unter http://www.datenschutz-berlin.de/jahresbe/04/anl/anlagenband2004.pdf (letzter Zugriff im Oktober 2007).

jedoch übertragbar sind an andere Nutzer[536] und nicht als starker Authentisierungsbeweis taugen. Ironischerweise werden diese Daten aber in vielen Fällen trotzdem mit anderen Datenbeständen verknüpft und sogar personenbezogen ausgewertet, wobei hier mit Wahrscheinlichkeiten gearbeitet wird, dass die Daten zum selben Betroffenen gehören.

Hier sollte bei einer Diensterbringung unter Pseudonym der Anbieter seinen Dienst so gestalten, dass Betroffene tatsächlich ihre Rechte wahrnehmen können, z.B. durch Anbieten von Accounts, bei deren Nutzung sich der Betroffene etwa durch ein Passwort authentisieren muss, oder durch sog. digitale Pseudonyme (vgl. unter Abschnitt 4.5.3.2), bei denen die Kenntnis eines geheimen Schlüssels die Zugehörigkeit zum Betroffenen nachweist. In jedem Fall müsste nicht nur über die eigentlichen Daten informiert werden, sondern auch über die Erkenntnisse, die aus den verketteten und angereicherten Informationen über den Betroffenen gewonnen werden. Auch dies geschieht heute allenfalls in Ausnahmefällen.

6.2.1.2 Steuerbarkeit

Will man Verketten unter Bedingungen stellen, ist nicht nur die Transparenz darüber wichtig, sondern die Akteure müssen auch ihre Anforderungen ausdrücken und – ggf. in Abstimmung mit den anderen Beteiligten – durchsetzen können. Basierend auf verkettungsarmen Strukturen können dann Steuerungsmöglichkeiten des Nutzers realisiert werden.

6.2.1.2.1 Verkettungsarme Strukturen

Da Entkettung von bereits verketteten Datenbeständen schwierig oder sogar unmöglich durchzusetzen ist, sollten die IT-Systeme und Prozesse grundsätzlich möglichst verkettungsarm gestaltet werden. Analog zu den Datenschutzprinzipien von Datensparsamkeit und Datenvermeidung kann man auch von Verkettungssparsamkeit und Verkettungsvermeidung sprechen.

Ebenso sollten bei der Technik- und Prozessgestaltung Entkettungsmöglichkeiten vorgesehen werden, was zumindest die Umsetzung von datenschutzrechtlich festgelegten Regelungen umfassen muss, z.B. indem auf Betroffenenreaktionen zur Korrektur oder Auflösung von Verkettung reagiert wird oder indem Daten wirksam gelöscht werden, sobald sie nicht mehr nötig sind.

Auch Workflows sollten separiert werden, so dass verschiedene Kennungen (Pseudonyme) für verschiedene Abläufe verwendet werden und so ein übergreifendes Verketten erschwert wird. Konzepte des „Identity Protectors“ (vgl. [Rossum/Gardeniers/Borking 1995], [Borking 1996]) sehen eine Aufteilung der Abläufe in sog. „Pseudonym-Domains“ (vgl. [IMS Study 2003]) vor. Auch ein Einbinden von Treuhändern kann der Separierung der Abläufe dienlich sein, damit übergreifende Verkettungen verhindert werden.

Wo die Zurechenbarkeit von Nutzern gegenüber anderen sichergestellt werden soll, sollten vertrauenswürdige dritte Stellen eingesetzt werden, die Unverkettbarkeit zwischen digitaler und realer Identität sicherstellen, solange diese Verkettung zur Zurechenbarkeit nicht erforderlich ist. Sie können Nutzern pseudonyme Beglaubigungen (vgl. 4.5.3.4) über ihre Eigenschaften oder Handlungen ausstellen, über deren Herausgabe der Nutzer dann die Kontrolle hat, wenn dies für eine seiner weiteren Aktionen erforderlich ist. Dies impliziert aber auch, dass Beglaubigungen (wie z.B. Zeitstempel) keine beliebig hohe Auflösung aufweisen sollten, um Nutzer nicht anhand ihrer pseudonymen Profile identifizieren zu können.

Dies gilt auch für explizite Reputation, die Nutzer in Form von Profilen über ihre bisherigen digitalen Aktionen aufbauen können. Hier müssen mehrseitig sichere Designoptionen von Reputationssystemen betrachtet werden, die zum einen die gewollte Verkettbarkeit von Aktionen im Sinne von Reputation erlauben und im Sinne negativer Reputation auch erzwingen, aber diese Aktionen nicht derart feingranular in der Reputation erfassen, dass eine ungewollte Verkettbarkeit zur realen Person oder auch nur eine Wiedererkennung durch andere möglich ist.

[536] Beispielsweise mit der Software „CookieCooker“ (http://www.cookiecooker.de/ (letzter Zugriff im Oktober 2007)).

Auch die Detailgenauigkeit bei RFID-Chips wäre vielfach nicht erforderlich und sollte vermieden werden, wenn es z.B. ausreicht, den Produkttyp zu kennzeichnen, und nicht jedes Exemplar mit einer eigenen eindeutigen Kennung versehen werden muss.

Ebenso ist der Aufbau von Adressen und Pseudonymen relevant für die anschließende Verkettungsmöglichkeit. Daher sollte bei der Systemgestaltung schon von Anfang an ein Augenmerk gelegt darauf werden, wie man Verkettungsmöglichkeiten einschränken kann, z.B. indem man die Kennungen sektorspezifisch einsetzt und änderbar macht. Anonymisierungsdienste für IP-Adressen und Cookies sollten Basisfunktionalität für die Internetnutzung sein, weil damit eine Verkettung auf diesen Ebenen erschwert wird. Authentizität, wo immer nötig, sollte stattdessen auf höheren Schichten mit starken Verfahren umgesetzt werden.

Wenn Nutzer selbst Pseudonyme bestimmen können, sollte ihnen bewusst gemacht werden, dass die Auswahl selbst ebenfalls Informationen beinhalten kann. In Online-Spielen können z.B. Listen von möglichen Vor- und Nachnamen vorgegeben werden, die den Nutzer in seiner Wahl einschränken und damit auch mögliche inhärente Informationen minimieren.

Überwachungsfreiheit von Räumen ließe sich durch Störsender (z.B. *Jammer*) unterstützen, die ein Heraussenden von Aufzeichnungen per Handy unterbinden würden.

6.2.1.2.2 Mehrseitig sichere Gestaltung von Systemen und Prozessen

Möglichkeiten zur Verkettungsvermeidung und -kontrolle sind auf Nutzerseite die Konzepte Privatheit fördernden, nutzergesteuerten Identitätsmanagements. Wünschenswert sind technische Systeme, die dies umsetzen. Wo diese nicht vorhanden sind, sollten Nutzer dazu animiert werden, für verschiedene Anwendungen bzw. in unterschiedlichen Kontexten, zwischen denen sie keine Verkettbarkeit wünschen, unterschiedliche Pseudonyme zu verwenden. Nutzer sollten jederzeit Kontrolle über ihre Daten haben und beeinflussen können, wer darauf Zugriff erhalten kann.

Wünschenswert wäre auch eine Funktionalität, die es erlaubt, standardmäßig aktivierte Geräte zeitweise zu deaktivieren. Dies sollte auch als physische Lösung (z.B. Schalter, um beispielsweise Mikrofon und Webcam definitiv abzuschalten) realisiert werden, um Nachteile von Software-Lösungen wie etwaige Fehlfunktion oder Bedienungsfehler zu vermeiden.

Damit nicht immer eine Interaktion mit dem Nutzer notwendig ist, sollten Geräte mit Policies entsprechend programmiert werden, in bestimmten Kontexten eine Verkettung oder Überwachung vorzunehmen oder nicht. Treffen mehrere Nutzer mit ihren Geräten aufeinander, so ist es erforderlich, dass ihre Geräte untereinander aushandeln, welche Policy zur Verkettung zur Geltung kommt.

Auf der Ebene von RFID-Chips sollten Betroffene die Möglichkeit haben, sich gegen ein unautorisiertes Auslesen zu schützen. Dazu sollte dem Betroffenen zumindest möglich sein, eine Lösch- oder „Kill-Funktion“ auf die RFID-Chips anzuwenden.

6.2.1.3 Qualitätssicherung

Gerade im Bereich der Verarbeitung personenbezogener Datenverarbeitung sollte Qualitätssicherung selbstverständlich sein. Dazu gehört nicht nur eine revisionssichere, nachvollziehbare Konzeption und Implementierung der Verarbeitungsverfahren, sondern auch die eingesetzten Algorithmen für Verkettung und verwendeten Modelle zur Auswertung sollten möglichst geringe Fehlerraten aufweisen. Dies gilt insbesondere dort, wo es zu einschneidenden Folgen, z.B. Diskriminierungen, Rufschädigungen oder finanziellen Schlechterstellungen, kommen kann. Selbst wenn das Datenschutzrecht nicht unmittelbar gilt, weil die verarbeiteten Daten nicht personenbezogen sind, ist entsprechende Sorgfalt geboten, sofern die Auswirkungen eben doch Personen beeinflussen und insoweit auch eine Verkettung vorliegt.

Für potenziell verkettungsstarke oder invasive Bereiche sollte eine Vorabkontrolle durchgeführt werden. Datenschutz-Gütesiegel und Datenschutz-Audit sollten zur Qualitätssicherung der Konzepte und IT-Produkte sowie des Betriebs der Systeme dienen.

Auch regelmäßige Prüfungen durch interne Datenschutzbeauftragte oder die zuständige Datenschutzaufsichtsbehörde sollten erleichtert werden, indem nicht ein Black Box-Betrieb vorgezeigt wird, sondern die einzelnen Komponenten sowie die Schnittstellen untereinander in ihrer datenschutzgerechten Funktionsweise geprüft werden können. Eine Modularisierung verringert die Komplexität und damit auch die Anfälligkeit für Fehler. Für Verkettung bedeutet dies insbesondere ein Abbilden des Datenflusses in den Phasen der Informationsanreicherung beginnend bei der gezielten Vergabe von Adressen und anderen Verkettungsmerkmalen bis hin zur Entscheidungsfindung. Auch Mechanismen zur Verbesserung der eingesetzten Algorithmen und Modelle sollten vorgesehen werden.

Für alle verarbeiteten Daten sollte garantiert sein, dass sie rechtmäßig verarbeitet werden. Werden Daten aus anderen Quellen genommen, muss dies ebenfalls rechtmäßig sein und dokumentiert werden. Technisch wäre dies implementierbar durch Privacy Policies oder allgemeiner Datenverarbeitungs-Policies, die direkt an die Daten gebunden sind (sog. „Sticky Policies“, vgl. [Karjoth/Schunter/Waidner 2002] und [Casassa Mont/Pearson/Bramhall 2003]) und auch bei Weitergabe der Daten daran gebunden bleiben [Leenes/Schallaböck/Hansen 2007]. Über alle Phasen der Informationsanreicherung müsste die entsprechende Dokumentation der Quellen und der jeweils verantwortlichen Ansprechpartner mitlaufen, damit Betroffene tatsächlich ihre Rechte wahrnehmen und mögliche Fehler wirklich aufgeklärt werden können.

6.2.2 Handlungsempfehlungen – Politik und Recht

6.2.2.1 Vertrauensbildende statt vertrauensschwächende Maßnahmen

Die Informationsgesellschaft wird nur dann funktionieren und ihr volles Potenzial ausschöpfen können, wenn

- für die Nutzer Transparenz besteht über geplante und mögliche Verkettungen ihrer Daten und
- es einen „Grundschutz“ sowohl für Datensicherheit als auch Datenschutz gibt, der für die Nutzer nicht viel zusätzlichen Aufwand oder Unbequemlichkeit bedeutet.

Maßnahmen für Transparenz sowie für diesen Grundschutz stärken das Vertrauen der Nutzer darin, dass sie eine aktive Teilhabe an der Informationsgesellschaft meistern können und ihre Rechte – wie in der Offline-Welt eingeübt – weiterhin wahrnehmen können. Dies betrifft im Besonderen die Nutzung von E-Government-Diensten.

Zurzeit werden in der Politik allerdings Ideen diskutiert, die mit einer Vertrauensschwächung in die Komponenten, die für eine Teilhabe an der Informationsgesellschaft nötig sind, einhergehen, allem voran die Online-Durchsuchung. Diese basiert auf Sicherheitslücken bei den technischen Geräten der zu Beobachtenden, die natürlich auch von nicht-staatlichen „Hackern“ ausgenutzt werden können. Hinzu kommt, dass bei typischen Infiltrationsmechanismen nicht auszuschließen ist, dass auch Unbeteiligte von der Maßnahme der Online-Durchsuchung betroffen werden. Daneben sind Informationen, die per Online-Durchsuchung gewonnen wurden, weniger verlässlich als auf herkömmlichem Weg gewonnene Daten [Hansen/Pfitzmann 2007] – insbesondere ist ihr Beweiswert vor Gericht fraglich. Insgesamt ist die Online-Durchsuchung ein Schritt in die falsche Richtung – insbesondere organisierte Kriminalität und Terroristen werden weit überdurchschnittlich gesicherte Rechner verwenden. Stattdessen sollten Datensicherheit und Datenschutz in der technischen Infrastruktur sowie im Bereich des technisch naiven Nutzers gestärkt werden.

6.2.2.2 Entwicklung von Anwendungen im eigenen Rechtsraum zum Schutz der Bürger

Ein erheblicher Teil von digitalen Identitäten wird außerhalb des deutschen oder auch europäischen Anwendungsbereichs der Datenschutzgesetze verarbeitet, d.h. gesammelt, verkettet und ausgewertet. Dies zeigt sich insbesondere an den großen US-amerikanischen Suchmaschinen, doch betrifft auch vielerlei Community-Dienste, Update-Server für Betriebssysteme oder Anwendungs-

software oder Systeme für Digital Rights Management. Selbst wenn diese Dienste – was in den meisten Fällen noch nicht der Fall ist – die Nutzer ausreichend aufklären und eine Einwilligung für die Verarbeitung der Daten einholen und selbst wenn sich diese Datenverarbeiter bemühen, ein – wie in der EU-Datenschutzrichtlinie 1995/46/EG gefordertes – angemessenen Schutzniveau zu garantieren, wären stets ein Zugriff und eine Auswertung durch die dort angesiedelten Behörden der nationalen Sicherheit möglich. Nicht nur aus Gründen des Datenschutzes, sondern auch in Bezug auf den Schutz von Betriebsgeheimnissen in Firmen oder eigene Anforderungen an nationale Sicherheit ist es riskant, dass all diese digitalen Identitäten außerhalb der deutschen (oder europäischen) Jurisdiktion verarbeitet werden, ohne dass eine angemessene Kontrolle ausgeübt werden kann.

Daher sollten den Nutzern alternative Anwendungen, z.B. für eine Suchmaschine, in Europa angeboten werden, die in Konkurrenz mit den bisher etablierten ausländischen Angeboten treten können. Hier müssten dann die europäischen Datenschutzvorgaben vorbildlich eingehalten werden. Dies würde auch die Autonomie des europäischen Staatenbundes fördern, der ebenfalls Interesse an Kontrolle der Verkettung von ihn betreffende Daten haben muss. Wo es um nationale – in Abgrenzung von europäischen – Interessen geht, müssten nationale Anwendungen bereitgestellt werden.

Im Beispiel der Suchmaschine würde es sogar ausreichen, für die Nutzung durch Europäer (und bei Bedarf auch andere Nutzer) vertrauenswürdig betriebene Proxies im europäischen Rechtsraum anzubieten, so dass eine nähere Auflösung der Requests bei ausländisch betriebenen Diensten nicht so einfach wäre. Noch besser wäre natürlich die Realisierung einer echten Anonymisierungsinfrastruktur (vgl. Abschnitt 4.5.1.2), statt sich auf wenige zentrale Proxies zu verlassen. Eine solche Anonymisierungsinfrastruktur wäre auch förderlich für den Schutz der Bürger im E-Government oder bei E-Democracy-Diensten wie E-Participation oder E-Voting.

6.2.2.3 Information der Öffentlichkeit über Verkettung bzw. Verkettbarkeit

Angesichts einer zunehmenden Anzahl von Datenbanken mit vielfach umfassenden Datenbeständen und immer einfacherer technischer Möglichkeiten für deren Verkettung erscheint eine umfassende Information der Menschen über bereits vorhandene und potenzielle Verkettungen sowie deren mögliche Auswirkungen als dringend geboten. Erforderlich ist eine grundsätzliche Sensibilisierung der Öffentlichkeit dafür, dass eine Verkettung digitaler Daten nicht nur Chancen bietet, sondern auch Risiken beinhaltet. Insoweit sollte den Menschen insbesondere vermittelt werden, wie leicht unter den Bedingungen der modernen Informationstechnik umfassende Persönlichkeitsprofile gebildet und ausgewertet werden können. Für interessierte Personen sollten Schulungen angeboten werden, in denen ein breiteres Wissen zu dieser Thematik vermittelt wird. Im Rahmen solcher Schulungen sollten insbesondere (technische) Möglichkeiten zur Kontrolle und Steuerung von Verkettung vorgestellt werden. Um einen möglichst großen Personenkreis zu erreichen, sollten solche Schulungsangebote in bereits bestehende gesellschaftliche Schulungskonzepte eingebunden werden. Zudem sollte es auch Schulungen für Technikentwickler und -gestalter geben, wodurch diese insbesondere für die Problematik unerwünschter Verkettungen sensibilisiert werden.

Die in Abschnitt 6.2.2.2 geforderten nationalen oder europäischen Anwendungen müssten Bestandteil des Schulungskonzeptes sein. So könnte in Schulen standardmäßig der Einsatz von Software, Suchmaschinen und Schutztools unterrichtet werden, die tatsächlich den Anforderungen an Verkettungssparsamkeit genügen.

6.2.2.4 Warnhinweise bezüglich Verkettung bzw. Verkettbarkeit

Zur Erhöhung der Transparenz sollte auf eine gesetzliche Verpflichtung hingewirkt werden, in Bedienungsanleitungen zu Produkten, bei deren Verwendung digitale Daten anfallen, Warnhinweise hinsichtlich möglicher Verkettungen dieser Daten aufzunehmen. Kombiniert werden könnten solche Angaben beispielsweise mit einer Veröffentlichung detaillierterer Informationen etwa auf Websites.

Auch die Privacy Policies für Websites sollten unter diesem Gesichtspunkt gestaltet werden (vgl. Abschnitt 6.2.1.1.2). In diesem Zusammenhang fällt auf, dass die EU-Datenschutzrichtlinie

1995/46/EG und ihre Umsetzung ins nationale Recht[537], z.B. das BDSG, lediglich ein Auskunftsrecht des Betroffenen auf Empfängerkategorien seiner übermittelten Daten, nicht jedoch auf die wirklichen Empfänger vorsieht. Dies ist aus Transparenzsicht unzureichend und sollte im Sinne des Betroffenen geändert werden.

6.2.2.5 Auflistung von Datenbanken, auf die staatliche Stellen zugreifen können

Die Transparenz für den Bürger sollte außerdem auch dadurch erhöht werden, dass eine Website eingerichtet wird, die einen vollständigen Überblick über bestehende staatliche Datenbanken gibt. Zudem sollte auf einer solchen Website auch darüber informiert werden, unter welchen Umständen staatliche Stellen auf private Datenbestände zugreifen dürfen und um welche (Arten von) Datenbanken es sich hier hauptsächlich handelt.

6.2.2.6 Festlegung von Best Practices

Eine Gefahr unerwünschter Datensammlung und Verkettung liegt in den vielfältigen und möglicherweise invasiven Auswertungsmöglichkeiten. Gerade für Marketingzwecke, die in den Datenschutzgesetzen privilegiert sind, könnten hier auch unethische – z.B. auf Manipulation zielende – Methoden zum Einsatz kommen. Tatsächlich weisen einige Unternehmen sogar im Kleingedruckten auf bestimmte Methoden hin, z.B. dass bei Flirt-SMS-Diensten die Kommunikationspartner nicht echt sind, doch dies wird von den Betroffenen oft übersehen, die ihren neuen „Bekanntschaften“ über Monate intime Details „simsen“. Stattdessen sollten die Unternehmen, die ethische Grundsätze einhalten, dies auch in Form einer Selbstverpflichtung öffentlich machen. Unternehmensverbände könnten zusammen mit Daten- und Verbraucherschützern Bedingungen für Verkettungen und Auswertungen erarbeiten und damit Standards schaffen.

6.2.2.7 (Mit-)Gestaltung von technischen Standards

Technische Standards haben vielfach sogar mehr Einfluss als nationales oder europäisches Recht. Beispiele für verkettungsrelevante internationale Standards sind

- die RFCs für das Internet-Protokoll einschließlich der Adressgestaltung (z.B. RFC 791 (Internet Protocol) und RFC 2460 (Internet Protocol, Version 6 (IPv6) Specification),
- die RFCs für das Domain Name System (DNS) (z.B. RFC 1034 (Domain Names – Concepts and Facilities) und RFC 1035 (Domain Names – Implementation and Specification)),
- die RFCs und W3C-Dokumente zu URIs, URLs und zur HTTP-Spezifikation inkl. Browser-Chatter (z.B. RFC 3986 (Uniform Resource Identifier (URI): Generic Syntax), RFC 1945 (Hypertext Transfer Protocol HTTP/1.0) und RFC 2616 (HTTP/1.1)),
- die RFCs und IETF-Dokumente zum Session Initiation Protocol (SIP) für IP-Telefonie (z.B. RFC 3261 – SIP: Session Initiation Protocol), oder auch
- die ICAO-Standardisierung im Bereich der maschinenlesbaren Reisedokumente (vgl. Abschnitt 3.2.4.2 zum Reisepass).

Obwohl in vielen Fällen Schwächen in den Standards bekannt und veröffentlicht sind, wirken sie weiterhin ein auf das tägliche Leben der Betroffenen durch – oft unnötige und intransparente – Verkettung von deren Daten. Beispielsweise wird für die Einführung des elektronischen Personalausweises in Deutschland argumentiert, dass man kompatibel sein möchte (oder sogar muss) zum Reisepass, dessen Spezifikation sich aus ICAO-Dokumenten ergibt – obwohl sich hier deutliche Probleme für die Datensicherheit der Passinhaber herausgestellt haben [Kosta et al. 2007].

[537] Zum Stand der Umsetzung der Datenschutzrichtlinie in nationales Recht der Mitgliedstaaten: [EU-Kommission 2007] und [EDPS 2007].

Hier scheint es noch stärker geboten als bisher, an den internationalen Standards mitzuwirken mit dem Ziel, Verkettungsmöglichkeiten zu erkennen, zu vermeiden oder zu gestalten. Solche Verkettungen und Verkettbarkeiten können sich beispielsweise aufgrund der jeweiligen Adressvergabe oder aufgrund von vorgesehenen oder auch nicht vorgesehenen, aber durch Datensicherheitsschwächen bedingt doch möglichen Zugriffsmöglichkeiten anderer auf die Daten ergeben. Die deutschen Datenschutzbeauftragten des Bundes und der Länder sowie die übrigen Aufsichtsbehörden im Datenschutzbereich haben heutzutage in der Regel weder die Ressourcen noch das Mandat dafür, an solchen internationalen Standardisierungen mitzuwirken.

6.2.2.8 Maßnahmen gegen das bestehende Vollzugsdefizit beim Datenschutz

Verstöße gegen Datenschutzbestimmungen kommen heute in vielen Fällen nicht an das Tageslicht oder ziehen nur selten spürbare Konsequenzen nach sich. Es sollte geprüft werden, ob eine Informationsverpflichtung der Unternehmen im Fall von folgenschweren Datenschutzverstößen oder Datensicherheitsmängeln analog zu den US-amerikanischen „Security Breach Notification Acts“ vorgesehen sein soll. Dies würde gleichermaßen die Transparenz gegenüber Betroffenen und die Disziplin der Unternehmen für eine rechtmäßige Datenverarbeitung erhöhen. Auch sollten Verstöße gegen Transparenzpflichten sanktioniert werden.

Die Beweislast für Rechtmäßigkeit der Datensammlung, Verkettung, Auswertung und Entscheidungsgenerierung liegt beim Datenverarbeiter. Auch beim Hinzuziehen von anderen Datenquellen, beim Einbinden von Auftragsdatenverarbeitern oder beim Auslagern von Datenbeständen auf Server im Ausland müssen die Rechtmäßigkeit der Verarbeitung sowie die Rechtewahrnehmung der Betroffenen sichergestellt sein. Dies sollte prüffähig, d.h. nachvollziehbar, dokumentiert sein (vgl. Abschnitt 6.2.1.3).

Die Datenschutzaufsichtsbehörden sollten dabei unterstützt werden, ausreichend tief gehende Prüfungen im komplexen Umfeld von Verkettung durchzuführen. Da bei diesen Prüfungen vielfach Expertenwissen vonnöten ist, sollten die Aufsichtsbehörden entsprechend ausgebildetes und befähigtes Personal erhalten.

6.2.2.9 Pseudonyme Signaturen politisch fördern statt hemmen

Auch wenn das Signaturgesetz die Möglichkeit einer Verwendung pseudonymer Signaturen ausdrücklich vorsieht, bestehen vielfältige tatsächlicher und rechtlicher Hemmnisse. So finden sich etwa im Bereich des Verwaltungsrechts gesetzliche Regelungen, die eine Verwendung pseudonymer Signaturen sehr stark einschränken. Zwar besteht in vielen Fällen ein legitimes Interesse des Staates an der Offenlegung der Identität eines Bürgers, jedoch sollte gründlich darüber nachgedacht werden, in welchen Fällen dies entbehrlich ist. Insbesondere könnten stattdessen Konzepte zum Einsatz kommen, die Anforderungen der Anonymität und Zurechenbarkeit kombinieren, z.B. sog. anonyme Credentials (vgl. Abschnitt 4.5.3.4). In einem zweiten Schritt sollten die gesetzlichen Regelungen dann so angepasst werden, dass die Verwendung pseudonymer Signaturen in den zuvor identifizierten Fällen ermöglicht wird.

6.2.2.10 Schaffung überwachungsfreier Räume

Nach dem heutigen Verständnis benötigen Menschen überwachungsfreie Räume für ihre Entwicklung zu selbstständig denkenden und entscheidenden Individuen. Das Bundesverfassungsgericht hat im Volkszählungsurteil 1983 festgestellt: „Die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen […] führen.“ In dieselbe Richtung argumentiert die ehemalige Präsidentin des Bundesverfassungsgerichtes, Prof. Dr. Jutta Limbach[538]: „Eine demo-

[538] Im Rahmen des Festvortrages des 53. Deutschen Anwaltstages am 10. Mai 2002 in München, siehe http://www.anwaltverein.de/downloads/stellungnahmen/2004-51.pdf (letzter Zugriff im Oktober 2007).

kratische politische Kultur lebt von der Meinungsfreude und dem Engagement der Bürger. Das setzt Furchtlosigkeit voraus. Diese dürfte allmählich verloren gehen, wenn der Staat seine Bürger biometrisch vermisst, datenmäßig durchrastert und seine Lebensregungen elektronisch verfolgt."

Solche überwachungsfreien Räume wären nicht auf den Schutz vor staatlichen Zugriffen beschränkt, sondern in einer Gesellschaft, in der fast jeder mit Fotohandy und anderen Alltagsgegenständen selbst zum Überwacher werden kann, wären auch Verabredungen sinnvoll, dass in bestimmten Räumlichkeiten nicht ausspioniert und aufgezeichnet wird. In diesem Sinn könnte ein „digitales Hausrecht" wirken, das auch mit technischer Unterstützung (z.B. Jammern) durchgesetzt werden könnte. Die Diskussion zu sog. „Digital Territories" (vgl. [Daskala/Maghiros 2007]) greift auf, das Verständnis von Räumen und Grenzen in Verbindung mit traditionellen Regeln des sozialen Verhaltens auf die digitale Welt zu übertragen.

6.2.2.11 Strafverfolgung: Lösungen für minimal-invasive Eingriffe

Gegenwärtig geht die Tendenz dahin, bereits im Gefahrenvorfeld Eingriffe in Grundrechte der Bürger zu ermöglichen. So verspricht man sich etwa von massenhaften Datenbevorratungen (Stichwort Vorratsdatenspeicherung) eine Effektivierung der Strafverfolgung. Insoweit dürfte aber das Gegenteil der Fall sein: Personen mit hoher krimineller Energie werden in vielen Fällen dazu in der Lage sein, auf solche neuen Informationsquellen für Strafverfolger zu reagieren. Überwiegend werden deshalb unbescholtene Bürger in das Visier der Strafverfolgungsbehörden geraten. Eine effektive Strafverfolgung sollte sich hingegen auf eine Überwachung bereits verdächtiger Personen konzentrieren, da dies bessere Ermittlungserfolge verspricht.

6.2.3 Handlungsempfehlungen – Forschung

In den vorigen Bereichen zur Technikgestaltung und zu Empfehlungen an Politik und Recht wurden Maßnahmen geschildert, die es unterstützen, Verkettungen unter Bedingung zu stellen. Vielfach sind die Maßnahmen noch nicht weit verbreitet im Einsatz, sondern es sind noch offene Fragen zu erforschen. Dies betrifft insbesondere Konzepte für nutzerkontrollierte Steuerung von Verkettung, das Identitätsmanagement, sowie die Ausgestaltung von Mechanismen zur Adressierungs-, Beobachtungs- und Verkettungsvermeidung. Wichtige Aspekte des weiteren Forschungsbedarfs werden in diesem Abschnitt skizziert.

6.2.3.1 Usability für Verkettungstransparenz und -steuerung

Die Forderung nach mehr Transparenz und Steuerbarkeit durch Betroffene kann nur sinnvoll umgesetzt werden, wenn die Betroffenen die Informationen auch tatsächlich verstehen und die technischen Systeme bedienen können. Die Komplexität der Technik und die Komplexität des Rechts dürfen nicht dazu führen, dass allenfalls noch Experten sich vor unerwünschter Verkettung schützen können. Aus diesem Grund sind einfache Bedienkonzepte für Steuerbarkeit von Verkettung und Verkettbarkeit zu entwickeln und an Nutzern auszutesten. Hierbei müssen neben Informatikern und Juristen auch Mediengestalter, Psychologen und Linguisten einbezogen werden.

6.2.3.2 Garantien vs. Ungewissheit

Eine Schutzmöglichkeit von Betroffenen in einer Welt, in der potenziell alle Informationen verkettet werden, besteht darin, ein Rauschen zu erzeugen, indem die relevanten Daten für Beobachter nicht mehr ersichtlich sind (vgl. Abschnitt 4.10 zu Entkettungsmechanismen). Dieses Rauschen könnte durch absichtliche Fehlinformation (Desinformation) erzeugt werden, die überall in der digitalen Welt auftauchen könnten, wo nicht besondere Authentizitätsanforderungen garantiert werden. Auch wenn die falschen Informationen nicht absichtlich, sondern versehentlich verbreitet werden (Miss-information), wäre zu untersuchen, wie sich dies auf die digitale Welt und vielleicht sogar auf die Gesellschaft auswirkt.

Je nach Bereich/Situation und Rolle der Beteiligten kann der Authentizitätsbedarf für anfallende Daten sehr unterschiedlich sein. In den Abschnitten 4.5.2 und 4.5.3 wurden Basistechniken vorgestellt, die für verschiedene Konstellationen unterschiedliche Authentikation ermöglichen.

Es wurde allerdings bisher nicht umfassend untersucht, in welchen Situationen welcher Authentizitätsbedarf besteht und inwieweit für alle sinnvollen Konstellationen bereits Techniken existieren. Es gibt also sowohl bezüglich der Klassifikation von Situationen hinsichtlich des Authentizitätsbedarfs als auch hinsichtlich der Entwicklung von Methoden zu dessen Erreichung weiterer Forschungsbedarf.

Die Diskussion sollte auch allgemeiner geführt werden: Welches Bedürfnis hat die Gesellschaft nach Garantien, z.B. für Verkettung (wenn es um Reputationssysteme geht, bei denen der Betroffene ihm nicht-genehme Bewertungen nicht entfernen können soll), für Nicht-Beobachtung (für überwachungsfreie Räume), für Unverkettbarkeit oder Anonymität (in bestimmten Bereichen, um eine Verkettung zu verhindern), für Zurechenbarkeit (um Verantwortung wahrzunehmen) oder für Authentizität (damit der Betroffene seine Datenschutzrechte wahrnehmen kann)? Welche Unschärfen will oder muss sich unsere Gesellschaft leisten (z.B. verdeckte Ermittler)?

6.2.3.3 Rechtliche Konzepte

Die heutigen rechtlichen Konzepte für Verkettungsregelungen basieren wie der Datenschutz auf gesetzlich festgelegter Rechtmäßigkeit oder informierter Einwilligung des Betroffenen. In beiden Bereichen besteht Forschungsbedarf:

- Die gesetzlichen Festlegungen sind in der Regel Datenverarbeitungsermächtigungen, die Konzepte zur Kombination von Anonymität und Zurechenbarkeit wie die Credentials nicht in Betracht ziehen. Hier wären in vielen Fällen daten- und verkettungssparsamere Umsetzungen möglich.
- Inwieweit das Einwilligungskonzept wirklich den Wunsch der Betroffenen widerspiegelt, ist zweifelhaft. Zumeist bestehen für den Betroffenen keine oder nur wenige Freiheitsgrade beim Einwilligen, wenn er nicht ganz auf den Dienst oder das Angebot verzichten will („Friss oder stirb“). Die Freiwilligkeit der Einwilligung steht dann in Frage. Während im persönlichen Gespräch oft noch Sonderregelungen vereinbart werden können, passiert dies bei vorgefertigten Vertragskomponenten nur selten, und in der digitalen Welt fehlt dann auch noch der persönliche Ansprechpartner. Hinzu kommt, dass die Information über die Datenverarbeitung – selbst wenn sie vorbildlich gegeben werden sollte – nicht immer beim Betroffenen ankommt. Zumindest dann, wenn der Betroffene nach dem Zurückziehen der Einwilligung weiter unter den Folgen leiden kann, ist eine Einwilligung offensichtlich nicht ausreichend.

Für den Bereich Transparenz fehlt es an Standards für Benachrichtigungspflichten und häufig auch an einer Verschränkung mit dem Online-Bereich: Insbesondere Funktionen zur Rechtewahrnehmung sollten für digitale Identitäten im Online-Bereich ermöglicht werden, so dass keine Hemmschwelle wegen eines Medienbruchs besteht. Die digitale Welt vereinfacht und verbilligt sogar vielfach das Informieren der Betroffenen, so dass hier gemeinsam von Juristen, Informatikern und Datenschutzaufsichtsbehörden Konzepte entwickelt werden sollten, die die Bürger und Verbraucher bei ihrer Rechtewahrnehmung unterstützen.

Zu prüfen wäre außerdem die Frage, ob aus den zunehmenden Kapazitäten zur Datenerhebung und -verarbeitung, die Privatpersonen mittlerweile zur Verfügung stehen, Handlungsbedarf für den Gesetzgeber resultiert. Schließlich können hier ebenfalls große Risiken für den Datenschutz der Mitmenschen bestehen; auf der anderen Seite kann zumindest bei der heutigen Gestaltung der IT-Systeme nicht erwartet werden, dass jeder Nutzer ein hohes Datensicherheitslevel garantiert.

6.2.3.4 Lenkung über Besteuerung oder Geldflüsse an den Betroffenen

Eine Möglichkeit für eine Lenkung durch den Staat ist Besteuerung, d.h. der Versuch der Regelung eines Sachverhaltes über Geld. Es wurde schon diskutiert, ob man Datenspeicher zusätzlich

besteuern soll, da sie ja die Basis für Datensammlung und damit die Basis für Verkettung und Auswertung darstellen. Dies scheint keine gute Idee zu sein, denn multimediale Daten benötigen sehr große Datenspeicher (z.B. digitale Filme), während sensible Daten ggf. nur wenige Byte groß sind. Eine Steuer an territorialen Grenzen, z.B. Exportkosten je nach Bandbreite, scheint aus demselben Grund nicht sinnvoll. Noch nicht zu Ende durchdacht ist der Vorschlag, das Auslesen von Identifiern für andere als den Betroffenen kostenpflichtig zu machen. Vielleicht wären Steuern der falsche Weg, und stattdessen müsste man den Geldfluss an den Betroffenen leiten. Ähnliches wäre dann im Bereich Erreichbarkeitsmanagement möglich: Bei einem unerwünschten Erreicht-Werden würden die Kosten für die Aufmerksamkeit des Angerufenen würden dem Anrufer in Rechnung gestellt. Hier können und sollen keine Handlungsempfehlungen ausgesprochen werden, aber ein Aufgreifen dieser Fragestellungen durch Forscher aus dem volkswirtschaftlichen und soziologischen Bereich wäre zu begrüßen.

Literaturverzeichnis

[*Abel 2006*] Abel, Ralf: Rechtsfragen von Scoring und Rating, in: Recht der Datenverarbeitung (RDV) 2006, S. 108 ff.

[*Ahlert/Backhaus/Meffert 2001*] Ahlert, Dieter/Backhaus, Kalus/Meffert, Heribert: Geschäftsmodelle im E-Business – Modethema oder mehr? (MCM-Studie zum Deutschen Marketing-Tag), 2001

[*AK-GG 2001*] Denninger, Erhard/Hoffmann-Riem, Wolfgang/Schneider, Hans-Peter/Stein, Ekkehart (Hrsg.): Alternativkommentar zum Grundgesetz für die Bundesrepublik Deutschland, Luchterhand, 3. Aufl., Neuwied 2001

[*Art. 29-Datenschutzgruppe 2004*] Art. 29-Datenschutzgruppe: Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten; abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_de.pdf (letzter Zugriff im Oktober 2007)

[*Art. 29-Datenschutzgruppe 2005*] Art. 29-Datenschutzgruppe: Datenschutzfragen im Zusammenhang mit der RFID-Technik; abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_de.pdf (letzter Zugriff im Oktober 2007)

[*Art. 29-Datenschutzgruppe 2007*] Art. 29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“; abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf (letzter Zugriff im Oktober 2007)

[*Asokan et al. 1997*] Asokan, N./Janson, Philippe A./Steiner, Michael/Waidner, Michael: The State of the Art in Electronic Payment Systems, in: IEEE Computer, September 1997, S. 28-35

[*Bauer/Meints/Hansen 2005*] Bauer, Matthias/Meints, Martin/Hansen, Marit (Hrsg.): FIDIS Deliverable D3.1 – Structured Overview on Prototypes and Concepts of Identity Management Systems, Frankfurt am Main 2005; abrufbar unter: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf (letzter Zugriff im Oktober 2007)

[*Bäumler 2003*] Bäumler, Helmut: Das Recht auf Anonymität, in: Bäumler, Helmut/von Mutius, Albert (Hrsg.), Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Vieweg Verlag, Braunschweig/Wiesbaden 2003, S. 1-11

[*Bausbach 2006*] Bausbach, Winfried: Fesseln für die wehrhafte Demokratie, in: Neue Juristische Wochenschrift (NJW) 2006, S. 1922 ff.

[*Berthold/Clauß 2007*] Berthold, Stefan/Clauß, Sebastian: Linkability Estimation Between Subjects and Message Contents Using Formal Concepts, angenommen bei DIM'07, ACM Workshop on Digital Identity Management, November 2007

[*Berthold/Pfitzmann/Standke 2000*] Berthold, Oliver/Pfitzmann, Andreas/Standke, Ronny: The disadvantages of free MIX routes and how to overcome them, in: Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability (PET) 2000, Springer Verlag, LNCS 2009, Juli 2000, S. 30-45

[*Bertsch et al. 1995*] Bertsch, Andreas/Damker, Herbert/Federrath, Hannes/Kesdogan, Dogan/Schneider, Michael J.: Erreichbarkeitsmanagement, in: Praxis der Informationsverarbeitung und Kommunikation 1995, S. 231 ff.

[*Bizer 2004*] Bizer, Johann: Personenkennzeichen, in: Datenschutz und Datensicherheit (DuD) 2004, S. 45 ff.

[*Böhme et al. 2004*] Böhme, Rainer/Danezis, George/Díaz, Claudia/Köpsell, Stefan/Pfitzmann, Andreas: On the PET Workshop Panel Mix Cascades Versus Peer-to-Peer: Is One Concept Superior?, in: Proceedings of Privacy Enhancing Technologies Workshop (PET) 2004, LNCS 3424, Springer Verlag, 2004

[Borcea-Pfitzmann et al. 2007] Borcea-Pfitzmann, Katrin/Hansen, Marit/Liesebach, Katja/Pfitzmann, Andreas/Steinbrecher, Sandra: Managing One's Identities in Organisational and Social Settings, in: Datenschutz und Datensicherheit (DuD) 2007, S. 671-675

[*Borking 1996*] Borking, John: Der Identity Protector, in: Datenschutz und Datensicherheit (DuD) 1996, S. 654 ff.

[*BSI 2004*] Bundesamt für Sicherheit in der Informationstechnik (BSI): Risiken und Chancen des Einsatzes von RFID-Systemen, 2004; abrufbar unter: http://www.bsi.de/fachthem/rfid/studie.htm (letzter Zugriff im Oktober 2007)

[*Camenisch/Lysyanskaya 2001*] Camenisch, Jan/Lysyanskaya, Anna: An efficient system for nontransferable anonymous credentials with optional anonymity revocation, in: EUROCRYPT ’01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Springer Verlag, London, UK, 2001, S. 93-118

[*Caplan 2001*] Caplan, Jane: "This or That Particular Person": Protocols of Identification in Nineteenth-Century Europe, in: Caplan, Jane/Torpey, John (Hrsg.), Documenting Individual Identity: The Development of State Practises in the Modern World, Princeton University Press, Princeton 2001, S. 49-66

[*Casassa Mont/Pearson/Bramhall 2003*] Casassa Mont, Marco/Pearson, Siani/Bramhall, Pete: Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services; abrufbar unter: http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf (letzter Zugriff im Oktober 2007)

[*CC 1998*] Common criteria for information technology security evaluation – part 2: Security functional requirements, Version 15408-2 FDIS, ISO/IEC SC27 N2162, 15. November 1998; abrufbar unter: http://www.bsi.de/cc/ (letzter Zugriff im Oktober 2007)

[*Chaum 1981*] Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM 24/2, 1981, S. 84-88

[*Chaum 1984*] Chaum, David: A New Paradigm for Individuals in the Information Age, 1984 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, Washington 1984, S. 99-103

[*Chaum 1984a*] Chaum, David: Design Concepts for Tamper Responding Systems, Crypto '83, Plenum Press, New York 1984, S. 387-392

[*Chaum 1985*] Chaum, David: Security Without Identification: Transaction Systems to Make Big Brother Obsolete, in: Communications of the ACM, Vol. 28 No. 10, S. 1030-1044, ACM, Oktober 1985

[*Chaum 1985a*] Chaum, David: The Dining Cryptographers Problem. Unconditional Sender Anonymity, Draft, 13. Mai 1985

[*Chaum 1988*] Chaum, David: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, in: Journal of Cryptology 1/1 (1988), S. 65-75

[*Chaum/Heyst 1991*] Chaum, David/Van Heyst, Eugéne: Group Signatures, in: D.W. Davies (Hrsg.), Advances in Cryptology – Eurocrypt ’91, LNCS 547, Springer Verlag, Berlin, 1991, S. 257-265

[*Chui/Zwick 1999*] Chui, Kevin/Zwick, Rami: Auction on the Internet – A Preliminary Study, Hong Kong University of Science and Technology, Marketing Working Paper Series, MKTG 99.132, 1999

[*Danezis 2003*] Danezis, George: Mix-Networks with Restricted Routes, in: Proceedings of Privacy Enhancing Technologies Workshop (PET) 2003, LNCS 2760, Springer Verlag, 2003

[*Daskala/Maghiros 2007*] Daskala, Barbara/Maghiros, Ioannis: D1gital Territ0ries – Towards the protection of public and private space in a digital and Ambient Intelligence environment, 22765 EN, Mai 2007; abrufbar unter: http://ftp.jrc.es/eur22765en.pdf (letzter Zugriff im Oktober 2007)

[*Däubler et al. 2007*] Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo: Bundesdatenschutzgesetz – Basiskommentar, Bund-Verlag, 2. Aufl., Frankfurt 2007

[*Dellarocas 2003*] Dellarocas, Chrysanthos: The digitization of word-of-mouth: Promise and challenges of online feedback mechanisms, Management Science, 2003

[*Denning 1982*] Denning, Dorothy E.: Cryptography and Data Security, Addison-Wesley, Reading, Mass., 1982

[*Díaz et al. 2002*] Díaz, Claudia/Seys, Stefaan/Claessens, Joris/Preneel, Bart: Towards measuring anonymity, in: Dingledine, Roger/Syverson, Paul (Hrsg.), Proceedings of Privacy Enhancing Technologies Workshop (PET 2002), LNCS 2482, Springer Verlag, 2002, S. 54-68

[*Durkheim 1984*] Durkheim, Emile: Die Regeln der soziologischen Methode, Suhrkamp, Frankfurt 1984

[*E-Participation-Studie 2006*] pol-di.net e.V. / politik-digital.de: Facilitating active citizenship – E-Participation in Großbritannien und Deutschland – Eine Bestandsaufnahme, Berlin 2006; abrufbar unter: http://www.britishcouncil.de/d/society/e_participation.htm (letzter Zugriff im Oktober 2007)

[*eBay 2005*] eBay: Annual report 2005; abrufbar unter: http://investor.ebay.com/annuals.cfm (letzter Zugriff im Oktober 2007)

[*Ebenroth/Boujong/Joost 2001*] Ebenroth, Carsten Thomas/Boujong, Karlheinz/Joost, Detlev (Hrsg.): Handelsgesetzbuch, Verlag C. H. Beck/Verlag Franz Vahlen, München 2001

[*Eckert 2006*] Eckert, Michael: Das allgemeine Gleichbehandlungsgesetz in der Praxis, in: Deutsches Steuerrecht (DStR) 2006, S. 1987 ff.

[*Eckhardt et al. 2000*] Eckhardt, Anne/Fattebert, Sylvain/Keel, Alois/Meyer, Patrick: Der Gläserne Kunde – Elektronische Erfassung und Auswertung von Kundendaten, Zentrum für Technologiefolgen-Abschätzung, Technology Assessment TA 38/2000, 2000

[*EDPS 2007*] Der Europäische Datenschutzbeauftragte: Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and theCouncil on the follow-up of the Work Programme for better implementation of the Data Protection Directive, 2007; abrufbar unter: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf (letzter Zugriff im Oktober 2007)

[*EICAR 2006*] EICAR Task Force on RFID: Leitfaden – RFID und Datenschutz, 2006; abrufbar unter: http://www.eicar.org/taskforces/rfid/RFID-Leitfaden-100406.pdf (letzter Zugriff im Oktober 2007)

[*Engel 2006*] Engel, Christian: Auf dem Weg zum elektronischen Personalausweis – Der elektronische Personalausweis (ePA) als universelles Identifikationsdokument, in: Datenschutz und Datensicherheit (DuD) 2006, S. 207 ff.

[*EU-Kommission 2007*] EU-Kommission: Mitteilung der Kommission an das Europäische Parlament und an den Rat – Stand des Arbeitsprogrammes für eine bessere Durchführung der Datenschutzrichtlinie (KOM/2007/87 endg.), 2007

[*Fahrmeier 2000*] Fahrmeier, Andreas: Citizens and Aliens. Foreigners and the Law in Britain and the German States, Berghahn Books, New York and Oxford 2000, S. 1789-1870

[*Feige 1990*] Feige, Uriel: Alternative Ways for Zero Knowledge Interactive Proofs, Dissertation, Weizmann Institute of Science, Rehovot, Israel, 1990

[*Finkenzeller 2006*] Finkenzeller, Klaus: RFID-Handbuch, Carl Hanser Verlag, München 2006

[*FIPS 1994*] FIPS-186 94: Digital signature standards. Federal Information Processing Standards Publication 186, U.S. Department of Commerce/N.I.S.T National Technical Information Services, Springfield 1994

[*Fischer-Hübner 2001*] Fischer-Hübner, Simone: IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, LNCS 1958, Springer Verlag, 2001

[*Fritsch et al. 2005*] Fritsch, Lothar/Roßnagel, Heiko/Schwenke, Matthias/Stadler, Tobias: Die Pflicht zum Angebot anonym nutzbarer Dienste – Eine technische und rechtliche Zumutbarkeitsbetrachtung, in: Datenschutz und Datensicherheit (DuD) 2005, S. 592 ff.

[*Frosch-Wilke 2003*] Frosch-Wilke, Dirk: Data Warehouse, OLAP und Data Mining – State of the Art und zukünftige Entwicklungen, in: Datenschutz und Datensicherheit (DuD) 2003, S. 597 ff.

[*Fuchs 2007*] Fuchs, Peter: Ethik und Gesellschaft – eine Vorlesung; abrufbar unter: http://www.fen.ch/texte/gast_fuchs_ethik.pdf (letzter Zugriff im Oktober 2007)

[*Garfinkel/Rosenberg 2005*] Garfinkel, Simson/Rosenberg, Beth: RFID – Applications, Security, and Privacy, Addison-Wesley, Amsterdam 2005

[*GI-Memorandum 2007*] Gesellschaft für Informatik e.V.: Memorandum der Gesellschaft für Informatik e.V. (GI) zur Identifizierung und Überwachung von Bürgern sowie der Beobachtung und Auswertung der Kommunikation, des Verhaltens, der Persönlichkeit und körperlicher Merkmale; abrufbar unter: http://www.gi-ev.de/fileadmin/redaktion/Download/GI-Memorandum_zur_Ueberwachung.pdf (letzter Zugriff im Oktober 2007)

[*Gola/Schomerus 2005*] Gola, Peter/Schomerus, Rudolf: Bundesdatenschutzgesetz – Kommentar, Verlag C. H. Beck, 8. Aufl., München 2005

[*Goldschlag/Reed/Syverson 1996*] Goldschlag, D. M./Reed, M. G./Syverson, P. F.: Anonymous Connections and Onion Routing, in: Proc. IEEE Symp. on Security and Privacy, Oakland, Mai 1997

[*Goldwasser/Micali/Rackoff 1985*] Goldwasser, Shafi/Micali, Silvio/Rackoff, Charles: The Knowledge Complexity of Interactive Proof-Systems, in: Proc. 17th STOC, ACM Press, 1985, S. 291-304

[*Golembiewski 2003*] Golembiewski, Claudia: Das Recht auf Anonymität im Internet – Gesetzliche Grundlagen und praktische Umsetzung, in: Datenschutz und Datensicherheit (DuD) 2003, S. 129 ff.

[*Gosewinkel 2001*] Gosewinkel, Dieter: Einbürgern und Ausschließen – Die Nationalisierung der Staatsangehörigkeit vom Deutschen Bund bis zur Bundesrepublik Deutschland, Vandenhoeck und Ruprecht Verlag, Göttingen 2001

[*Graevenitz 2006*] Graevenitz, Gerik: Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren, LIT Verlag, Berlin 2006

[*Groebner 2004*] Groebner, Valentin: Der Schein der Person – Steckbrief, Ausweis und Kontrolle im Mittelalter, Verlag C. H. Beck, München 2004

[*Gundermann 2003*] Gundermann, Lukas: Sozialhilfe für Dagobert Duck – Sind Anonymität und Pseudonymität im E-Government möglich?, in: Datenschutz und Datensicherheit (DuD) 2003, S. 282-286

[*Günther 1978*] Günther, Gotthard: Beiträge zur Grundlegung einer operationsfähigen Dialektik, 1. bis 3. Band, Felix Meiner Verlag, Hamburg 1978

[*Hagel/Armstrong 1997*] Hagel, John/Armstrong, Arthur G.: Net Gain: Expanding Markets Through Virtual Communities, Harvard Business School Press, 1997

[*Hallaschka/Jandt 2006*] Hallaschka, Florian/Jandt, Silke: Standortbezogene Dienste im Unternehmen, in: Multimedia und Recht (MMR) 2006, S. 436 ff.

[*Hansen/Borcea-Pfitzmann/Pfitzmann 2005*] Hansen, Marit/Borcea-Pfitzmann, Katrin/Pfitzmann, Andreas: PRIME – Ein europäisches Projekt für nutzerbestimmtes Identitätsmanagement, it – Information Technology, Oldenbourg 47/6 (2005) S. 352-359

[*Hansen/Meints 2006*] Hansen, Marit/Meints, Martin: Digitale Identitäten – Überblick und aktuelle Trends: Identity-Lifecycle, Authentisierung und Identitätsmanagement, in: Datenschutz und Datensicherheit (DuD) 2006, S. 543 ff.

[*Hansen/Meissner 2007*] Hansen, Markus/Meissner, Sebastian: Identification and Tracking of Individuals and Social Networks using the Electronic Product Code on RFID Tags, in: Proceedings of IFIP & FIDIS Summer School in Karlstad, IFIP International Federation for Information Processing (im Erscheinen), 2008; Vorversion von 2007 online abrufbar unter http://www.cs.kau.se/IFIP-summerschool/IFIP2007/papers/S03_P2_Markus%20Hansen.pdf (letzter Zugriff im Oktober 2007)

[*Hansen/Pfitzmann 2007*] Hansen, Markus/Pfitzmann, Andreas: Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme, Deutsche Richterzeitung, August 2007, S. 225-228

[*Hansen/Rost 2003*] Hansen, Marit/Rost, Martin: Nutzerkontrollierte Verkettung – Pseudonyme, Credentials, Protokolle für Identitätsmanagement, in: Datenschutz und Datensicherheit (DuD) 2003, S. 293 ff.

[*Heng 2007*] Heng, Stefan: eCommerce mit etablierten Bezahlsystemen arrangiert, Deutsche Bank Research, Mai 2007

[*Hildebrandt 2006*] Hildebrandt, Mireille: Profiling: From Data to Knowledge – The challenges of a crucial technology, in: Datenschutz und Datensicherheit (DuD) 2006, S. 548 ff.

[*Hildebrandt/Backhouse 2005*] Hildebrandt, Mireille/Backhouse, James (Hrsg.): FIDIS Deliverable 7.2 – Descriptive analysis and inventory of profiling practises, Frankfurt am Main 2005; abrufbar unter: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.2.profiling_practices.pdf (letzter Zugriff im Oktober 2007)

[*Höckel 1985*] Höckel, Gunter: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen, Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, August 1985

[*Höckel/Pfitzmann 1985*] Höckel, Gunter/Pfitzmann, Andreas: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen, 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer Verlag, Berlin 1985, S. 113-127

[*Hoffmann-Riem 2002*] Hoffmann-Riem, Wolfgang: Freiheit und Sicherheit im Angesicht terroristischer Anschläge, in: Zeitschrift für Rechtspolitik (ZRP) 2002, S. 497 ff.

[*Hofstadter 1985*] Hofstadter, Douglas R.: Gödel, Escher, Bach – Ein Endloses Geflochtenes Band, dtv, München 1985

[*Hopp/Grünvogel 2002*] Hopp, Claudia/Grünvogel, Andreas: Pseudonyme nach dem deutschen und österreichischen Signaturgesetz – Datenschutzrechtliche Aspekte rechtsvergleichend betrachtet, in: Datenschutz und Datensicherheit (DuD) 2002, S. 79 ff.

[*Hoppe 2004*] Hoppe, Tilman: Bildaufnahmen aus dem höchstpersönlichen Lebensbereich – der neue § 201a StGB, in: Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2004, S. 990 ff.

[*Hoppenstedt 2004*] Hoppenstedt, Dietrich H.: Unser Umgang mit Geld muss sich immer auch an den sozialen und gesellschaftlichen Folgen messen lassen, in: Kreditwesen 24/2004, S. 27

[*Hornung 2006*] Hornung, Gerrit: Elektronische Zertifikate, Ausweise und Pseudonyme – Voraussetzungen der Selbstbestimmung, in: Roßnagel, Alexander (Hrsg.), Allgegenwärtige Identifizierung? Neue Identitätsinfrastrukturen und ihr rechtliche Gestaltung, Nomos Verlagsgesellschaft, Baden-Baden 2006, S. 53-69

[*Hu et al. 2007*] Hu, Jian/Zeng, Hua-Jun/Li, Hua/Niu, Cheng/Chen, Zheng: Demographic Prediction Based on User's Browsing Behavior; abrufbar unter: http://www2007.org/papers/paper686.pdf (letzter Zugriff im Oktober 2007)

[*Huberman/Franklin/Hogg 1999*] Hubermann, Bernardo A./Franklin, Matt/Hogg, Tad: Enhancing privacy and trust in electronic communities, ACM Conference on Electronic Commerce, 1999, S. 78-86

[*Hughes/Shmatikov 2004*] Hughes, Dominic/Shmatikov, Vitaly: Information Hiding, Anonymity and Privacy: A Modular Approach, in: Journal of Computer Security, 12(1), 2004, S. 3-36

[*IMS Study 2003*] Hansen, Marit/Krasemann, Henry/Krause, Christian/Rost, Martin/Genghini, Riccardo: Identity Management Systems (IMS): Identification and Comparison Study, 2003; abrufbar unter: https://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf (letzter Zugriff im Oktober 2007)

[*Info-RFID 2006*] Informationsforum RFID: RFID im Gesundheitswesen; abrufbar unter: http://www.info-rfid.de/downloads/rfid_im_gesundheitswesen.pdf (letzter Zugriff im Oktober 2007)

[*Jandt 2007*] Jandt, Silke: Datenschutz bei Location Based Services – Voraussetzungen und Grenzen der rechtmäßigen Verwendung von Standortdaten, in: Multimedia und Recht (MMR) 2007, S. 74 ff.

[*Kang/Lee 2005*] Kang, Seo-Il/Lee, Im-Yeong: A Study on the E-Cash System with Anonymity and Divisibility, ICCSA (2) 2005, S. 177-186

[*Karjoth/Schunter/Waidner 2002*] Karjoth, Günter/Schunter, Matthias/Waidner, Michael: Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data, LNCS, Springer Verlag, 2002

[*Keller 1990*] Keller, Rolf: Das Phänomen der vorbeugenden Bekämpfung von Straftaten, in: Neue Zeitschrift für Strafrecht (NStZ) 1990, S. 416 ff.

[*Kellner 2007*] Kellner, Martin: Die E-Petition zum Bundestag: Ein Danaergeschenk, in: Neue Justiz (NJ) 2007, S. 56 ff.

[*Kohlheim 2005*] Kohlheim, Rosa/Kohlheim, Volker: Duden Familiennamen – Herkunft und Bedeutung von über 20.000 Nachnamen, Bibliographisches Institut & F.A. Brockhaus AG, 2. Aufl., Mannheim 2005

[*Köhntopp/Köhntopp 2000*] Köhntopp, Marit/Köhntopp, Kristian: Datenspuren im Internet, in: Computer und Recht (CR) 2000, S. 248-257

[*Köhntopp/Pfitzmann 2000*] Köhntopp, Marit/Pfitzmann, Andreas: Datenschutz Next Generation, in: Bäumler, Helmut (Hrsg.), E-Privacy, Vieweg, Wiesbaden 2000, S. 316-322

[*Kollock 1999*] Kollock, Peter: The production of trust in online markets, Advances in Group Processes (Vol. 16), Greenwich, CT: JAI Press., 1999

[*Kosta et al. 2007*] Kosta, Eleni/Meints, Martin/Hansen, Marit/Gasson, Mark: An analysis of security and privacy issues relating to RFID enabled ePassports, in: Venter, Hein/Eloff, Mariki/Labuschagne, Les/Eloff, Jan/Solms, Rossouw von (Hrsg.), New Approaches for Security, Privacy and Trust in Complex Environments, Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), Springer Verlag, New York 2007, S. 467-472

[*Kotschy 2006*] Kotschy, Waltraut: Die Bürgerkarte in Österreich – Identity management im E-Government, in: Datenschutz und Datensicherheit (DuD), 2006, S. 201 ff.

[*Krasemann 2006*] Krasemann, Henry: Onlinespielrecht – Spielwiese für Juristen, in: Multimedia und Recht (MMR) 2006, S. 351 ff.

[*Krasemann 2006a*] Krasemann, Henry: Selbstgesteuertes Identitätsmanagement – Rechtliche Möglichkeiten der Nutzung verschiedener Identitäten, in: Datenschutz und Datensicherheit (DuD) 2006, S. 211 ff.

[*Krings 2004*] Krings, Günter: Die Petitionsfreiheit nach Art. 17 GG, in: Juristische Schulung (JuS) 2004, S. 474 ff.

[*Kutscha 2003*] Kutscha, Martin: Rechtsschutzdefizite bei Grundrechtseingriffen von Sicherheitsbehörden, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2003, S. 1296 ff.

[*Leenes/Schallaböck/Hansen 2007*] Leenes, Ronald/Schallaböck, Jan/Hansen, Marit (Hrsg.): PRIME White Paper V2, 27. Juni 2007; abrufbar unter: https://www.prime-project.eu/prime_products/whitepaper/ (letzter Zugriff im Oktober 2007)

[*Luhmann 1991*] Luhmann, Niklas: Soziologie des Risikos, Berlin, 2003 (Erstausgabe 1991)

[*Luhmann 1997*] Luhmann, Niklas: Die Gesellschaft der Gesellschaft, Suhrkamp, Frankfurt am Main 1997

[*Mahler/Olsen 2004*] Mahler, Tobias/Olsen, Thomas: Reputation systems and data protection law, in: eAdoption and the Knowledge Economy: Issues, Applications, Case Studies, Amsterdam, IOS Press 2004, S. 180-187

[*Manturana 1982*] Manturana, Humberto: Erkennen: Die Organisation und Verkörperung von Wirklichkeit – ausgewählte Schriften zur biologischen Epistemologie, Vieweg, Braunschweig/Wiesbaden 1982

[*Märker 2005*] Märker, Oliver: Online-Mediation als Instrument für eine nachhaltige Stadt und Regionalplanung. eine qualitative Untersuchung zur internen und externen Relevanz online-mediierter Verfahren, Shaker Verlag, Aachen 2005

[*Märker/Trénel 2003*] Märker, Oliver/Trénel, Matthias (Hrsg.): Online-Mediation. Neue Medien in der Konfliktvermittlung – mit Beispielen aus Politik und Wirtschaft, Edition Sigma, Berlin 2003

[*Markus 2002*] Markus, Ursula: Integration der virtuellen Community in das CRM, Josef Eul Verlag, 2002

[*Mattern 2007*] Mattern, Friedemann: Allgegenwärtige Informationsverarbeitung – Technologietrends und Auswirkungen – Ubiquitous Computing, 2007; abrufbar unter: http://www.vs.inf.ethz.ch/publ/papers/AllgegenwInfoverarb.pdf (letzter Zugriff im Oktober 2007)

[*Mead 1934*] Mead, G.H.: Mind, Self, and Society, edited by Charles W. Morris, Chicago, 1934

[*Medert/Süßmuth 2005*] Medert, Klaus M./Süßmuth, Werner: Melderecht des Bundes und der Länder I. Bundesrecht, Deutscher Gemeindeverlag, 22. Ergänzungslieferung, Schwerin 2005

[*Meints/Hansen 2006*] Meints, Martin/Hansen, Marit (Hrsg.): FIDIS Deliverable 3.6 – Study on ID Documents, Version 1.1, Frankfurt am Main 2006; abrufbar unter: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.6.study_on_id_documents.pdf (letzter Zugriff im Oktober 2007)

[*Meyer-Goßner 2005*] Meyer-Goßner, Lutz: Strafprozessordnung – Mit GVG und Nebengesetzen, Verlag C. H. Beck, 48. Aufl., München 2005

[*Möllers 2000*] Möllers, Christoph: Polizeikontrollen ohne Gefahrverdacht – Ratio und rechtliche Grenzen der neuen Vorsorgebefugnisse, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2000, S. 382 ff.

[*Moos 2004*] Moos, Peter von (Hrsg.): Unverwechselbarkeit. Persönliche Identität und Identifikation in der vormodernen Gesellschaft, Böhlau Verlag, Köln 2004

[*Moos 2006*] Moos, Flemming: Unzulässiger Handel mit Persönlichkeitsprofilen? – Erstellung und Vermarktung kommerzieller Datenbanken mit Personenbezug, in: Multimedia und Recht (MMR) 2006, S. 718 ff.

[*Mutius 2003*] von Mutius, Albert: Anonymität als Element des allgemeinen Persönlichkeitsrechts – terminologische, rechtssystematische und normstrukturelle Grundfragen, in: Bäumler, Helmut/von Mutius, Albert (Hrsg.), Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Vieweg Verlag, Braunschweig/Wiesbaden 2003, S. 12-26

[*Neumann 2003*] Neumann, Heike: Anonyme Zahlungssysteme – Bezahlen ohne seinen guten Namen, in: Datenschutz und Datensicherheit (DuD) 2003, S. 270 ff.

[*Nolde/Leger 2002*] Nolde, Veronika/Leger, Lothar (Hrsg.): Biometrische Verfahren, Fachverlag Deutscher Wirtschaftsdienst, Köln 2002

[*Paaß/Wauschkuhn 1984*] Paaß, Gerhard/Wauschkuhn, Udo: Datenzugang, Datenschutz und Anonymisierung – Analysepotential und Identifizierbarkeit von anonymisierten Individualdaten, Oldenbourg, München 1984

[*Petri 2007*] Petri, Thomas B.: Informationsverarbeitung im Polizei- und Strafverfahrensrecht, in: Lisken, Hans/Denninger, Erhard, Handbuch des Polizeirechts – Gefahrenabwehr, Strafverfolgung, Rechtsschutz, Verlag C. H. Beck, 4. Aufl., München 2007, S. 825-1007

[*Pfeiffer 2003*] Pfeiffer, Gerd (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz mit Einführungsgesetz, Verlag C. H. Beck, 5. Aufl., München 2003

[*Pfitzmann 1985*] Pfitzmann, Andreas: How to implement ISDNs without user observability – Some remarks, Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 14/85

[*Pfitzmann 1986*] Pfitzmann, Andreas: Die Infrastruktur der Informationsgesellschaft: Zwei getrennte Fernmeldenetze beibehalten oder ein wirklich datengeschütztes errichten?, in: Datenschutz und Datensicherheit (DuD) 1986, S. 353 ff.

[*Pfitzmann/Hansen 2007*] Pfitzmann, Andreas/Hansen, Marit: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Draft v0.29, 31. Juli 2007); abrufbar unter: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (letzter Zugriff im Oktober 2007)

[Phillips 2004] Phillips, David J.: Privacy policy and PETs – The influence of policy regimes on the development and social implications of privacy enhancing technologies, in: New Media & Society, SAGE Publications, London, Thousand Oaks, CA and New Delhi, Vol. 6(6), 2004, S. 691-706

[*Pommerening 1991*] Pommerening, Klaus: Datenschutz und Datensicherheit, BI-Wissenschaftsverlag, Mannheim, Wien, Zürich 1991

[*Popek/Kline 1978*] Popek, Gerald J./Kline, Charles S.: Design Issues for Secure Computer Networks, Operating Systems, An Advanced Course, edited by R. Bayer, R. M. Graham, G. Seegmüller, LNCS 60, 1978, nachgedruckt als Springer Study Edition, 1979, Springer Verlag, Heidelberg, S. 517-546

[*Poscher 2001*] Poscher, Ralf: Der Gefahrverdacht – Das ungelöste Problem der Polizeirechtsdogmatik, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2001, S. 141 ff.

[*Rheingold 1993*] Rheingold, Howard: Virtual Community, HarperTrade, 1993

[*Rivest/Shamir/Adleman 1978*] Rivest, R. L./Shamir, A./Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21/2 (1978) S. 120-126, nachgedruckt: 26/1 (1983) S. 96-99

[*Roberto 2002*] Roberto, Vito: Rückrufe von Personenwagen und Kostentragung (Info-Tech, Expose II), November 2002

[*Roggan/Bergemann 2007*] Roggan, Fredrik/Bergemann, Nils: Die "neue Sicherheitsarchitektur" der Bundesrepublik Deutschland – Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz, in: Neue Juristische Wochenschrift (NJW) 2007, S. 876 ff.

[*Rohwer et al. 2006*] Rohwer, Thomas/Tolkmit, Carsten/Hansen, Marit/Hansen, Markus/Möller, Jan/Waack, Henning: White Paper: Abwehr von "Spam over Internet Telephony" (SPIT-AL), Kiel, 31.01.2006; abrufbar unter: http://www.spit-abwehr.de/Whitepaper_SPITAL_20060310.pdf (letzter Zugriff im Oktober 2007)

[*Roßnagel 2002*] Roßnagel, Alexander: Der elektronische Ausweis – Notwendige und mögliche Identifizierung im E-Government, in: Datenschutz und Datensicherheit (DuD) 2002, S. 281 ff.

[*Roßnagel 2003*] Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, Verlag C. H. Beck, München 2003

[*Roßnagel 2007*] Roßnagel, Alexander: Datenschutz in einem informatisierten Alltag, Friedrich-Ebert-Stiftung, Berlin 2007

[*Roßnagel et al. 2006*] Roßnagel, Alexander/Jandt, Silke/Müller, Jürgen/Gutscher, Andreas/Heesen, Jessica (Hrsg.): Datenschutzfragen mobiler kontextbezogener Systeme, DuD-Fachbeiträge, DUV-Verlag, Wiesbaden 2006

[*Roßnagel/Pfitzmann/Garstka 2001*] Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001

[*Roßnagel/Scholz 2000*] Roßnagel, Alexander/Scholz, Philip: Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, in: Multimedia und Recht (MMR) 2000, S. 721 ff.

[*Rossum/Gardeniers/Borking 1995*] Rossum, Henk van/Gardeniers, Huib/Borking, John et al.: Privacy-enhancing Technologies, The path to anonymity, Volume I u. II, Achtergrondstudies en Verkenningen 5b, Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Canada, August 1995

[*Rost 2003*] Rost, Martin: Über die Funktionalität von Anonymität für die bürgerliche Gesellschaft, in: Bäumler, Helmut/von Mutius, Albert (Hrsg.), Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Vieweg, Braunschweig/Wiesbaden 2003, S. 62-72

[*Rost 2004*] Rost, Martin: Verkettbarkeit als Grundbegriff des Datenschutzes – Identitätsmanagement soziologisch beobachtet, in: Bizer, Johann/von Mutius, Albert/Petri, Thomas B./Weichert, Thilo, Innovativer Datenschutz 1992-2004 – Wünsche, Wege, Wirklichkeit – Für Helmut Bäumler, Selbstverlag ULD, Kiel 2004, S. 315-334

[*Sachs 2003*] Sachs, Michael (Hrsg.): Grundgesetz, Verlag C. H. Beck, 3. Aufl., München 2003

[*Schaar 2001*] Schaar, Peter: Persönlichkeitsprofile im Internet, in: Datenschutz und Datensicherheit (DuD) 2001, S. 383 ff.

[*Schaar 2005*] Schaar, Peter: Informationsverbund der europäischen Sicherheitsbehörden – wo bleibt der Datenschutz? Dokumentation zur Konferenz des Deutschen Instituts für Menschenrechte, 2005

[*Schaar 2006*] Schaar, Peter: Datenaustausch und Datenschutz im Vertrag von Prüm, in: Datenschutz und Datensicherheit (DuD) 2006, S. 691 ff.

[*Scheja 2005*] Scheja, Gregor: Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank Dissertation, Nomos Verlagsgesellschaft, Baden-Baden 2005

[*Schmid 2006*] Schmid, Helmut: Chipmigration: Hauptargument Vertrauen, in: cards Karten cartes 2006, S. 26 ff.

[*Schmitz 2003*] Schmitz, Heribert: Einlegung einer Petition durch E-Mail?, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2003, S. 1437 ff.

[*Schneider/Sidiropoulos 1996*] Schneider, Steve/Sidiropoulos, Abraham: CSP and Anonymity, in: ESORICS 1996, LNCS 1146, Springer Verlag, Berlin, 1996, S. 198-218

[*Schnorr 1991*] Schnorr, C.: Efficient signature generation by smart cards, in: Journal of Cryptology 4/3 (1991), S. 161-174

[*Schuppan/Reichard 2002*] Schuppan, Tino/Reichard, Christoph: eGovernment: Von der Mode zur Modernisierung, in: Landes- und Kommunalverwaltung (LKV) 2002, S. 105 ff.

[*Serjantov/Danezis 2002*]: Serjantov, Andrei/Danezis, George, Towards an Information Theoretic Metric for Anonymity, in: R. Dingledine, P. Syverson (Hrsg.), Proceedings of Privacy Enhancing Technologies Workshop (PET 2002), LNCS 2482, Springer Verlag, 2002, S. 41-53

[*Shannon 1948*] Shannon, Claude E.: A Mathematical Theory of Communication, The Bell System Technical Journal, 27, 1948, S. 379-423, S. 623-656

[*Simitis 2006*] Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, Nomos Verlagsgesellschaft, 6. Aufl., Baden-Baden 2006

[*Stahl et al. 2005*] Stahl, Ernst/Krabichler, Thomas/Breitschaft, Markus/Wittmann, Georg: Sichere Zahlungsverfahren für E-Government, ibi Research an der Universität Regensburg, 2005

[*Stahl et al. 2006*] Stahl, Ernst/Krabichler, Thomas/Breitschaft, Markus/Wittmann, Georg: Zahlungsabwicklung im Internet – Bedeutung, Status-Quo und zukünftige Herausforderungen, Regensburg 2006

[*Steinbrecher 2006*] Steinbrecher, Sandra: Design options for privacy-respecting reputation systems within centralized Internet communities, Proceedings of 21st IFIP International Information Security Conference “Security and Privacy in Dynamic Environments”, IFIP 201, Springer Verlag, 2006

[*Steinbrecher/Köpsell 2003*] Steinbrecher, Sandra/Köpsell, Stefan: Modelling Unlinkability, in: R. Dingledine (Hrsg.), Proceedings of Privacy Enhancing Technologies workshop (PET 2003), LNCS 2760, Springer Verlag, 2003, S. 32-47

[*Steininger/Neun/Edwardes 2006*] Steininger, Stefan/Neun, Moritz/Edwardes, Alistair: Foundations of Location Based Services, 2006; abrufbar unter: http://www.geo.unizh.ch/publications/cartouche/lbs_lecturenotes_steinigeretal2006.pdf (letzter Zugriff im Oktober 2007)

[*Steinmüller et al. 1971*] Steinmüller, W./Lutterbeck, B./Mallmann, C./Harbort, U./Kolb, G./Schneider, J.: Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, 1971

[*Stubblebine/Syverson 1999*] Stubblebine, Stuart G./Syverson, Paul F.: Fair on-line auctions without special trusted parties, 3rd International Conference on Financial Cryptography (FC ’99), LNCS 1648, Springer Verlag, Berlin 1999, S. 230-240

[*Sweeney 2002*] Sweeney, Latanya: k-Anonymity: A Model for Protecting Privacy, in: International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 2002, S. 557-570

[*Syverson/Stubblebine 1999*] Syverson, Paul F./Stubblebine, Stuart G.: Group Principals and the Formalization of Anonymity, Proceedings of the World Congress on Formal Methods (1), 1999, S. 814-833

[*Tanenbaum 1981*] Tanenbaum, Andrew S.: Computer Networks, Prentice-Hall, Englewood Cliffs, N. J., 1981

[*TAUCIS 2006*] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)/Humboldt-Universität Berlin (HU): TAUCIS – Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (Studie im Auftrag des Bundesministeriums für Bildung und Forschung); abrufbar unter: https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf (letzter Zugriff im Oktober 2007)

[*Thiel 2006*] Thiel, Jürgen: Elektronische Identifizierung und Authentifizierung im E-Government, in: Roßnagel, Alexander (Hrsg.), Allgegenwärtige Identifizierung?, Nomos Verlagsgesellschaft, Baden-Baden 2006, S. 47-52

[*Thome 2005*] Thome, Rainer: eGovernment – Entwicklungsstand und Potenziale, in: Datenverarbeitung – Steuer – Wirtschaft – Recht (DSWR) 2005, S. 205 ff.

[*Tinnefeld/Ehmann/Gerling 2005*] Tinnefeld, Marie-Theres/Ehmann, Eugen/Gerling, Rainer W.: Einführung in das Datenschutzrecht, Oldenbourg Wissenschaftsverlag, 4. Aufl., München 2005

[*ULD-Kundenbindungsstudie 2003*] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): Kundenbindungssysteme und Datenschutz, Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V., 2003; abrufbar unter: https://www.datenschutzzentrum.de/wirtschaft/Kundenbindungssysteme.pdf (letzter Zugriff im Oktober 2007)

[*ULD-Scoring-Gutachten 2006*] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): Scoringsysteme zur Beurteilung der Kreditwürdigkeit, Scoring-Gutachten für das Bundesverbraucherministerium, 2006; abrufbar unter: http://www.bmelv.de/nn_752314/SharedDocs/downloads/02-Verbraucherschutz/Finanzdienstleistungen/scoring,templateId=raw,property=publicationFile.pdf/scoring.pdf (letzter Zugriff im Oktober 2007)

[*ULD-Verbraucherdatenschutz-Studie 2006*] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, 2006; abrufbar unter: https://www.datenschutzzentrum.de/verbraucherdatenschutz/ (letzter Zugriff im Oktober 2007)

[*Voydock/Kent 1983*] Voydock, Victor L./Kent, Stephen T.: Security Mechanisms in High-Level Network Protocols, in: ACM, Computing Surveys, ACM, 1983, S. 135-171

[*Warg 2006*] Warg, Gunter: Auskunftsbefugnisse der Strafverfolgungsbehörden und Anonymität des E-Mail-Anzeigeerstatters, in: Multimedia und Recht (MMR) 2006, S. 77 ff.

[*Wearden 2004*] Wearden, Graeme: Judge raps ebay over fraud, 7. Dezember 2004; abrufbar unter: http://news.com.com/Judge+raps+eBay+over+fraud/2100-1038_3-5481601.html?tag=item (letzter Zugriff im Oktober 2007)

[*Weichert 1996*] Weichert, Thilo: Datenschutzrechtliche Probleme beim Adresshandel, in: Wettbewerb in Recht und Praxis (WRP) 1996, S. 522 ff.

[*Weichert 2002*] Weichert, Thilo: Die Wiederbelebung des Personenkennzeichens – insbesondere am Beispiel der Einführung einer einheitlichen Wirtschaftsnummer, in: Recht der Datenverarbeitung (RDV) 2002, S. 170 ff.

[*Weichert 2006*] Weichert, Thilo: Verbraucher-Scoring meets Datenschutz, in: Datenschutz und Datensicherheit (DuD) 2006, S. 399 ff.

[*Weiser 1991*] Weiser, Mark: The Computer for the Twenty-First Century, 1991; abrufbar unter: http://www.ubiq.com/hypertext/weiser/UbiHome.html (letzter Zugriff im Oktober 2007)

[*Wesel 2006*] Wesel, Uwe: Geschichte des Rechts – Von den Frühformen bis zur Gegenwart, Verlag C. H. Beck, 3. Aufl., München 2006

[*White 2001*] White, Nancy: Community member roles and types, 2001; abrufbar unter: http://www.fullcirc.com/community/memberroles.htm (letzter Zugriff im Oktober 2007)

[*Wolf/Pfitzmann 2000*] Wolf, Gritta/Pfitzmann, Andreas: Properties of protection goals and their integration into a user interface, in: Computer Networks 32 (2000), S. 685-699

[*ZSI 1989*] Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitskriterien – Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT), Bundesanzeiger, Köln 1989

Abkürzungsverzeichnis

@	at
§	Paragraf
§§	Paragrafen
60er	sechziger
90er	neunziger
AAA	Authentication, Authorization, Accounting
AAL	Ambient Assisted Living
a.a.O.	am angegebenen Orte
ABMG	Autobahnmautgesetz
Abs.	Absatz
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeinen Gleichbehandlungsgesetz
AHV	Alters- und Hinterlassenenversicherung
AmI	Ambient Intelligence
AN.ON	Anonymität.Online
AO	Abgabenordnung
AOL	America Online
Art.	Artikel
AufenthG	Aufenthaltsgesetz
B2B	Business-to-Business
B2C	Business-to-Consumer
BAF	Bundesamt für Finanzen
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
Blog	Weblog
BMF	Bundesministerium für Finanzen
bPK	bereichsspezifische(s) Personenkennzeichen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
bzgl.	bezüglich
BZSt	Bundeszentralamt für Steuern
bzw.	beziehungsweise
C2C	Consumer-to-Consumer
ca.	circa
Captcha	Completely Automated Public Turing test to tell Computers and Humans Apart
CCTV	Closed Circuit Television
CD	Compact Disk
Cell-ID	Cell of Origin

CRM	Customer Relationship Management
CSP	Communicating Sequential Processes
DART	Dynamic Advertising, Reporting, and Targeting (Technik der Firma DoubleClick)
DCC	Direct Client-to-Client
DC-Netz	Dining-Cryptographers-Netz
ders.	derselbe
d.h.	das heißt
dies.	dieselben
DIN	Deutsches Institut für Normung e.V.
DNA	Desoxyribonukleinsäure
DNS	Domain Name System
DuD	Datenschutz und Datensicherheit
E-Administration	elektronische Administration
EAG	Europarechtsanpassungsgesetz
EC-Karte	Electronic-Cash-Karte
E-Commerce	Electronic Commerce
E-Democracy	Electronic Democracy
EDI	Electronic Data Interchange – elektronischer Datenaustausch
EDV	Elektronische Datenverarbeitung
EFF	Electronic Frontier Foundation
EG	Europäische Gemeinschaften
E-Government	Electronic Government
E-Identity	Electronic Identity
Einl.	einleitend
E-Justice	Electronic Justice
E-Mail	Electronic Mail
engl.	englisch
EOTD	Enhanced Observed Time Difference
E-Participation	Electronic Participation
EPC	Electronic Product Code
E-Petition	Electronic Petition
E-Plate	Electronic Plate – Nummernschild mit RFID
et al.	et alii – und weitere
etc.	et cetera
EU	Europäische Union
EUCARIS	European Car Information System
EUR	Euro
EURODAC	Europäisches dactyloskopisches System
e.V.	eingetragener Verein
E-Voting	Electronic Voting
EWR	Europäischer Wirtschaftsraum
f.	folgende
Fa.	Firma
ff.	fortfolgende
FIDIS	Future of Identity in the Information Society (EU-Projekt 2004-2009)

Fn.	Fußnote
g	Gramm
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
G2N	Government-to-Non-Governmental Organization
GB	Gigabyte
gem.	gemäß
Gestapo	Geheime Staatspolizei
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GHz	Gigahertz
GKV	gesetzliche Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GO SH	Gemeindeordnung für Schleswig-Holstein
GPS	Global Positioning System
griech.	griechisch
HF	Hochfrequenzbereich
HGB	Handelsgesetzbuch
H.M.	herrschende Meinung
HS	Halbsatz
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IC3	Internet Crime Complaint Center
ICAO	International Civil Aviation Organisation
ID	Identifikation, Identifikationsnummer
i.d.R.	in der Regel
IEC	International Electrotechnical Commission – Internationale elektrotechnische Kommission
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMS	Identity Management System
Inc.	Incorporated
IOI	Item of Interest
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization – Internationale Organisation für Normung
IT-System	Informationstechnik-System
ITU-T	International Telecommunication Union – Internationale Fernmeldeunion
IuK-Technologie	Informations- und Kommunikationstechnologie
i.V.m.	in Verbindung mit
JAP	Client-Software des Anonymisierungssystems AN.ON

Kap.	Kapitel
Kfz	Kraftfahrzeug
KG	Kommanditgesellschaft
km/h	Kilometer pro Stunde
KNN	künstliche neuronale Netze
KrO SH	Kreisordnung für Schleswig-Holstein
KUG	Kunsturhebergesetz
KWG	Kreditwesengesetz
lat.	lateinisch
LBS	Location Based Service(s)
LDSGe	Landesdatenschutzgesetze
LDSG SH	Landesdatenschutzgesetz Schleswig-Holstein
LKW	Lastkraftwagen
LMG SH	Landesmeldegesetz Schleswig-Holstein
LVwG SH	Landesverwaltungsgesetz Schleswig-Holstein
m	Meter
MDStV	Mediendienste-Staatsvertrag
Mhz	Megahertz
mm	Millimeter
MMS	Multimedia Messaging Service
MMOG	Massive-Multiplayer-Online-Game
MP3	MPEG-1 Audio Layer 3
MPEG	Moving Picture Experts Group
MRRG	Melderechtsrahmengesetz
MRZ	Machine Readable Zone
m.w.N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
NstZ	Neue Zeitschrift für Strafrecht
Nr.	Nummer
NS	Nationalsozialismus
OLAP	On-line Analytical Processing
OSCI	Online Services Computer Interface
OWiG	Ordnungswidrigkeitengesetz
P2P	Peer-to-Peer
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
PKZ	Personenkennzeichen
PRIME	Privacy and Identity Management for Europe (EU-Projekt 2004-2008)
PStG	Personenstandsgesetz
PStRG	Personenstandsreformgesetz
QoS	Quality of Service
RSA	Rivest – Shamir – Adleman (asymmetrischer Verschlüsselungsalgorithmus)
RFC	Request for Comments
RFID	Radio Frequency Identification

RISER	Registry Information Service on European Residents
Rn.	Randnummer
RSS	Really Simple Syndication, RDF Site Summary oder Rich Site Summary (News-Feed-Format)
RStV	Rundfunkstaatsvertrag
S.	Seite
SGB I	Erstes Buch Sozialgesetzbuch
SGB V	Fünftes Buch Sozialgesetzbuch
SGB X	Zehntes Buch Sozialgesetzbuch
SigG	Signaturgesetz
SILC	Secure Internet Live Conferencing
SIP	Session Initiation Protocol
SIS	Schengener Informationssystem
SMS	Short Message Service
SOCKS	SOCKetS (Internet-Proxy-Protokoll)
sog.	so genannte/r/s/m/n
SPIT	Spam over Internet Telephony
SSN	Social Security Number
SSL	Secure Socket Layer
StGB	Strafgesetzbuch
StIdV	Steueridentifikationsnummerverordnung
StPO	Strafprozessordnung
SWAMI	Safeguards in a World of Ambient Intelligence (EU-Projekt 2005-2006)
TCP	Transmission Control Protocol
TDG	Teledienstegesetz
TDDSG	Teledienstedatenschutzgesetz
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOA	Time of Arrival
u.a.	unter anderem
u.Ä.	und Ähnliches
UHF	Ultrahochfrequenzbereich
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
URI	Universal Resource Identifier
URL	Uniform Resource Locator
USA	Vereinigte Staaten von Amerika
USB	Universal Serial Bus
u.U.	unter Umständen
UUID	Universally Unique Identifier
VAbstG SH	Volksabstimmungsgesetz Schleswig-Holstein
Var.	Variante
vgl.	vergleiche
VIS	Visa Information System
VKVV	Verordnung über die Versicherungsnummer, die Kontoführung und den Versicherungsverlauf in der gesetzlichen Rentenversicherung

VL-AG	Verkettungs-Logistik Aktiengesellschaft (fiktive Firma in einem Szenario)
vs.	versus
VwVfG	Verwaltungsverfahrensgesetz
W3C	World Wide Web Consortium
Well	Whole Earth 'Lectronic Link
WLAN	Wireless Local Area Network
WWW	World Wide Web
XML	Extensible Markup Language
X.509v3	Version 3 von X.509 (ITU-T-Standard für eine Public-Key-Infrastruktur)
z.B.	zum Beispiel
ZensVorbG	Zensusvorbereitungsgesetz
ZEVIS	Zentrales Verkehrsinformationssystem
ZfdG	Zollfahndungsdienstgesetz
ZMR	Zentrale Melderegisternummer
z.T.	zum Teil