Privatheit

Privatheit umfasst viele Bereiche des menschlichen Lebens, weshalb die Definitionen von Privatheit auch sehr unterschiedlich sind. Eine bekannte Definition stammt von Louis D. Brandeis:

> *„[Privacy is] The right to be left alone" [WaBr80].*

Privatheit oder das Recht auf informationelle Selbstbestimmung ist ein Grundbedürfnis des Menschen. Jeder Mensch hat das Interesse, bestimmte Bereiche seines Lebens nicht seiner Umwelt offen zu legen. So ist auch in den Menschenrechten das Recht auf Privatheit verankert:

> *„No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, …" [UnNa48].*

Das Bundesverfassungsgericht befasste sich 1983 aufgrund der Volkszählung mit Privatheit und definierte das Recht auf informationelle Selbstbestimmung als die „*Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen*". Für die digitale Wirtschaft ist vor allem die Verarbeitung und Weitergabe von Daten relevant, die man schützen möchte. Alan F. Westin definierte Privatheit als:

> *„the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others, …"* [West67].

Privatheit teilt sich in zwei Bereiche auf, die unterschiedliche Maßnahmen zum Schutz der Privatheit erfordern [TaMo01]:

Zugriffskontrolle: Sind personenbezogene Daten im System des Nutzers gespeichert, so dürfen nur Berechtigte Zugriff auf diese Daten haben.

Verwertung der Daten: Sind personenbezogene Daten an Dritte übermittelt worden, so hat der Nutzer oft technisch keinen Einfluss mehr auf diese Daten. Es muss trotzdem gewährleistet werden, dass diese Daten nicht entgegen dem Wunsch des Nutzers ausgewertet, verändert oder weitergegeben werden.

Zugriffskontrolle liegt im Einflussbereich des Nutzers. Um Zugriffskontrolle zu erzielen, muss das System benutzbar und sicher sein, d.h. adäquate Zugriffsmechanismen bereitstellen und die Daten sicher speichern. Dafür müssen die Schutzziele der mehrseitigen Sicherheit durchgesetzt werden und eine verständliche Benutzungsoberfläche existieren. Zugriffskontrolle wird generell mit technischen Maßnahmen realisiert. Diese beinhalten einerseits Kontrollmechanismen auf dem System des Nutzers, aber auch Schutzmechanismen in anderen genutzten Systemen. So kann beispielsweise ein Anonymitätsdienst im Netz entstehende System- und Protokolldaten innerhalb einer großen Anonymitätsmenge vermischen, verschleiern oder durch andere Mechanismen eine Analyse behindern. Identitätsmanagement erlaubt dem Nutzer den situationsabhängigen Wechsel seiner (Netz-)Identität, wodurch er sich verschiedenen Kommunikationspartnern gegenüber unterschiedlich identifizieren kann.

Nachdem personenbezogene Daten das System des Nutzers verlassen haben, liegt die Verwertung der Daten beim Kommunikationspartner und nicht mehr im Einflussbereich des Nutzers. Entsprechend greifen auch rein technische Maßnahmen nicht mehr, mit denen der Nutzer seine Daten verändern oder löschen könnte. Zur Kontrolle der Verwertung der personenbezogenen Daten bedarf es zusätzlich nicht-technischer Maßnahmen wie beispielsweise dem Datenschutzgesetz, mit denen die Verwertung von personenbezogenen Daten gesetzlich gesteuert wird [RoPG02].

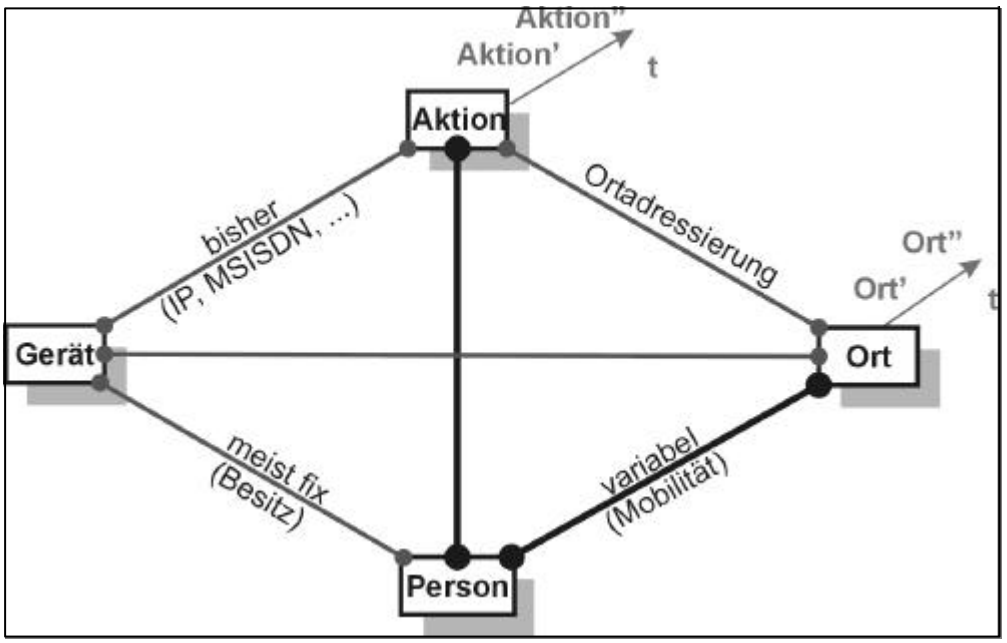

Abbildung: Das Freiburger Privatheitsviereck

Die Problematik allgemein, aber auch die Schwierigkeiten der technischen Realisierung von Privatheit lassen sich am Freiburger Privatheitsviereck [MuKZ01] (siehe Abbildung) verdeutlichen. Es definiert als relevante Entitäten zum Schutz der Privatheit: Nutzer, Ort, Gerät und Aktion. Zu jedem Zeitpunkt, zu dem eine Aktion getätigt wird, entsteht der folgende Zusammenhang: Eine Person führt an einem Ort mit einem Gerät eine Aktion durch. Die Privatsphäre der Person wird dann berührt, wenn die Beziehung zwischen Person und Aktion (Anonymität) oder die Beziehung zwischen Person und Aufenthaltsort aufgedeckt wird und zwar gegen den Willen der betroffenen Person. Die Aufdeckung dieser Beziehung muss durch das Zusammenwirken von technischen und nicht-technischen Maßnahmen unterbunden werden. So kann ein Nutzer beispielsweise die Verbindung „Gerät – Person" unterbrechen, wenn er in einem Internet-Café E-Mails schreibt. Die Nutzung von Anonymisierern unterbricht die Verbindung „Gerät – Aktion", da durch den Anonymisierer gerätespezifische Daten wie IP-Adressen oder Betriebssysteminformationen herausgefiltert oder verschleiert werden.

Literatur:

[MuKZ01] *Müller, G./ Kreutzer, M./ Zugenmaier, A.*: Location Adressing: Technical Paradigm for Privacy and Security in a Ubiquitous World, Hitachi Report 9/2001, Tokyo, 2001.

[RoPG02] *Roßnagel, R./ Pfitzmann, A./ Garska, H. J.*: Modernisierung des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin: 2002.

[TaMo01] *Tavani, H. T./ Moor, J. H.*: Privacy Protection, Control of Information, and Privacy-Enhancing Technologies, in: ACM SIGCAS Newsletter, Vol. 31, No. 1, 2001, S. 6-11.

[UnNa48] *General Assembly of the United Nations*: Universal Declaration of Human Rights, 1948. URL: http://www.un.org/Overview/rights.html. Zuletzt aufgerufen am: 02.07.2002.

[WaBr80] *Warren, S. D./ Brandeis, L. D.*: The Right to Privacy, in: Harvard Law Review, Vol. 4, No. 5, 1880.

[West67] *Westin, A. F.*: Privacy and Freedom, New York: Atheneum, 1967.

Auszug aus:

Günter Müller, Torsten Eymann, Michael Kreutzer:

Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft,

Lehrbücher Wirtschaftsinformatik, Oldenbourg Verlag, 2002, ISBN 3-486-25888-5