Soziale Netze und die Individualisierung der IT als Datenschutzproblem

Jessica Heesen[1], Martin Neubauer[2]

Institut für Philosophie[1]
Universität Stuttgart
Seidenstraße 36
70174 Stuttgart
jessica.heesen@philo.uni-stuttgart.de

Institut für Kommunikationsnetze und Rechnersysteme[2]
Universität Stuttgart
Pfaffenwaldring 47
70569 Stuttgart
martin.neubauer@ikr.uni-stuttgart.de

Abstract: Soziale Netze entsprechen dem Trend einer Individualisierung der Mediennutzung. Dieser Trend ist ambivalent: implizite Erwartungen in Bezug auf Individualisierung wie Selbstbestimmungsfähigkeit oder Personalisierung der Anwendungen stehen Risiken für den Persönlichkeitsschutz und der Überwachung gegenüber. Der Beitrag analysiert Aspekte der Individualisierung von Informations- und Kommunikationstechniken und diskutiert Problemlagen sowie Lösungsansätze in Hinsicht auf eine Informationelle Selbstbestimmung.

1 Individualisierung und Humanzentrierung als Zukunftsvision

Gemäß den Leitvorstellungen und Zukunftsvisionen von IT-Branche und Entwicklern wendet sich die Informations- und Kommunikationstechnik mit einer in der Technikgeschichte noch nicht bekannten Intensität den einzelnen Techniknutzern zu. „In the future, computation will be human-centered. It will be freely available everywhere, like batteries and power sockets, or oxygen in the air we breathe." [MIT04]. Ein Baustein dieser Entwicklung sind die Sozialen Netze, die sich zurzeit noch stark auf das Internet beziehen. In Zukunft werden sie sich als Möglichkeit der individuellen Selbstdarstellung mit den Informationsnetzwerken in intelligenten Umgebungen verbinden. In diesbezüglichen Szenarien zum Ubiquitous oder Pervasive Computing [ISTAG01] und im Web 2.0 wird die Individualität der Nutzerinnen und Nutzer in besonderer Weise hervorgehoben.

Im Folgenden wird dargestellt, inwiefern implizite Wertannahmen in Bezug auf Individualisierung mit der expliziten technischen Ausgestaltung des Personenbezugs in Konflikt geraten. Im Vordergrund steht dabei die individualrechtliche Verankerung der Informationellen Selbstbestimmung in Relation zum Umgang mit kollektiven Daten in digitalen sozialen Netzen.

2 Individualisierung und Informationelle Selbstbestimmung

Der Gedanke der Individualität jedes Menschen beinhaltet ein freiheitliches und gleichzeitig normatives Ideal: das der Selbstzweckhaftigkeit des Menschen und seiner Fähigkeit, sich als autonome Existenz selbst zu bestimmen. Insofern wird die Konzentrierung auf die Individualität der Nutzer als Form der *Humanisierung* verstanden. Gesellschaftlich wird die Förderung der Individualisierung in der Regel als Indiz und Ermöglichungsgrund für eine freiheitliche Gesellschaftsordnung, für Wahl- und Handlungsfreiheit gewertet. Aus dem Gedanken der Autonomie ist auch das Recht auf Privatheit zu verstehen. Autonomie kann sich nur in einem von Beobachtung und Fremdbestimmung freien Raum entfalten [vgl. Rö01, S. 138]. Die Verwirklichung eines Privatbereichs ist im Kontext der Nutzung von sozialen Netzen von Widersprüchen gekennzeichnet: Einerseits unterstützen soziale Netze und personalisierte Dienste insbesondere private Handlungen. Andererseits führt die Publizität der privaten Handlungen zur Aushöhlung der Bedingungen für die Entstehung einer Privatsphäre. Diese notwendigen Bedingungen sind an die Möglichkeit der Abgrenzung eines privaten Raums, privater Handlungsentscheidungen und Daten gegenüber Anderen gebunden.
Der Begriff des Privaten ist ebenso wie der der informationellen Selbstbestimmung verbunden mit einer *Kontrolle* über personenbezogene Informationen. Hier geht es nicht nur darum, dem Individuum Abwehrrechte in Bezug auf persönliche Daten zuzusichern, sondern – und das ist für das Informationsmanagement in sozialen Netzen von besonderer Bedeutung – es geht auch darum, Information und Kommunikation für Formen der *Identitätsausbildung gestalten* zu können: „Die informationelle Selbstbestimmung schützt … die selbstbestimmte Entwicklung und Entfaltung des Einzelnen. Diese kann nur in einer für ihn kontrollierbaren Selbstdarstellung in unterschiedlichen sozialen Rollen und der Rückspiegelung durch die Kommunikation mit anderen gelingen“ [Ro06]. Umgekehrt werden auch neue Möglichkeiten geboten, die Identitäten *Anderer* mitzubestimmen. Offene Plattformen wie soziale Netze können nicht nur Identitäten formen, sie können auch Existenzen gefährden. In offenen Plattformen kann jeder ohne intensive Kontrolle beliebige technische Bezeichner (wie z.B. URLs, Email-Adressen etc.) beantragen und beliebige Inhalte bereitstellen. Wer einer Person schaden will, kann falsche Inhalte einstellen. Ein Beispiel für Vorstufen solcher Möglichkeiten sind gezielte Negativeintragungen über Lehrer in Bewertungssystemen wie „Spick Mich“. Warum haben die Schüler nicht eine Homepage für den Lehrer eingerichtet und ihn dort mit falschen Angaben „bedacht“? Diese Problematik wird dadurch verschärft, dass Personalabteilungen schon heute das Internet über die Bewerber „ausgoogeln“. Wer dann mit falschen Informationen präsent ist oder auch nur versehentlich mit einer anderen Person verwechselt wird, bekommt eventuell aus diesem Grund die gewünschte Stelle nicht. Zudem trifft bereits heute die Aussage „Das Netz vergisst nichts!“ näherungsweise zu.

3 Grenzen der Nutzerkompetenz und notwendiges Systemvertrauen

Die Individualisierung von Netzdiensten führt zu einer anspruchsvollen Verwaltung von Zugangsdaten und Nutzerpräferenzen. Bisher verwaltet praktisch jeder Dienstanbieter

seine Nutzer selbst und fordert damit von jedem Nutzer einen eigenen Zugang. Ein Nutzungszugang kann hierbei als Partielle Digitale Identität [PH07] aufgefasst werden. Das heißt, Pseudonymisierung mit voller Nutzerkontrolle ist bereits Praxis. Typischerweise erfordert jeder Nutzungszugang ein Nutzername-Passwort-Paar zur Authentisierung und Autorisierung. Dieser Ansatz führt mit steigender Anzahl beanspruchter Dienste zur unweigerlichen Steigerung der Anzahl Nutzername-Passwort-Paare, die sich ein Nutzer einprägen muss. Dies ist bereits heutzutage nicht nutzerfreundlich und führt mit der zu erwartenden Etablierung allgegenwärtiger IT zu wachsenden Schwierigkeiten. Die bisherige Praxis verschärft den Trend zur Wiederverwendung von wenigstens den Passworten und unterläuft damit den gewünschten Grad an Sicherheit (Identity Theft).

Auf diese Probleme reagieren technologische Entwicklungen, die eine Vereinheitlichung und organisationsübergreifende Verwaltung von Nutzungszugängen zum Ziel haben (Federated Identity Management). Zum Beispiel soll mittels Single-Sign-On ein Nutzer sein Nutzername-Passwort-Paar nur einmal eingeben müssen, um unterschiedliche Dienste verschiedener, kooperierender Dienstanbieter nutzen zu können. Dabei spielt die Auslagerung der Nutzerverwaltung und Nutzerdatenbank aus dem eigentlichen Dienst in eine separate Komponente (Identity Provider) eine wichtige Rolle. Die separate Komponente kann mittels standardisierter Schnittstellen auf die Nutzerdatenbank, z.B. in Form von Directory-Services zugreifen. Diese Auslagerung erlaubt die organisationsübergreifende Zusammenschaltung und Zentralisierung der Nutzerdatenbank.

Solche Ansätze können die Anzahl Nutzername-Passwort-Paare wieder reduzieren, sofern die involvierten Dienstanbieter die Auslagerung zum einen technologisch unterstützen und zum anderen in die Auslagerung zum Identity Provider vertrauen. Vertrauen kann hierbei unterschiedlichste Formen annehmen. Zum Beispiel kann Vertrauen auf schriftlichen Verträgen basieren (kommerzielle Ausprägung) aber auch bis hin zu keinerlei Zusagen (Community Ausprägung) reichen. Beispiele für erstgenannte sind Systeme gemäß Liberty Alliance und Shibboleth, für letztgenannte LightWeight Identity und OpenID. Vor allem OpenID erfährt momentan eine gewaltige Stärkung durch große kommerzielle Unternehmen (Microsoft, Yahoo, Google) und besitzt das Potenzial, der zukünftige Standard im Internet zu werden.

Das Problem der Wahrung der Informationellen Selbstbestimmung wird dadurch verschärft, dass technologisch sehr vielschichtige (Vielfalt der Informationsarten), umfangreiche (große Menge an Werten einer veränderlichen Information, z.B. Ort) und akkurate (technologisch begründete Genauigkeit bei sensorischen Daten) *Nutzerprofile* erstellt werden können. Durch Zentralisierung ergänzen sich gegebenenfalls dezentral entstandene Teilprofile, wodurch ein Ort höchster Anreicherung personenbezogener Daten entsteht.

Faktisch muss jeder Nutzer der Technik und dem Betreiber vertrauen, da eine technologisch durchgesetzte externe Überprüfbarkeit nicht sichergestellt werden kann. Ein Nutzer erhält nur insoweit in fremdbetriebene Datenbanken Einblick, wie der Betreiber dazu willens ist. Zudem ist der Vorteil digitaler Systeme, die einfache und billige Vervielfältigung von Information, hier ein Nachteil. Falls bei Einsichtnahme das Datum tatsächlich nicht mehr gefunden wird, kann die Information in einer versteckten Datenbank oder gar bei Dritten verfügbar sein.

4 Individueller Besitz von Daten

Der Fokus Informationeller Selbstbestimmung liegt auf Informationen, die einen eigenständigen Wert bezüglich der Privatheit und/oder Selbstbestimmung einer Person besitzen. Damit stehen Daten, die entweder unmittelbar bei der Erfassung oder zu einem späteren Zeitpunkt einen Bezug zu wenigstens einem Individuum aufweisen im Zentrum. Aufgrund dieses Personenbezugs von Besitz zu sprechen, erscheint zunächst natürlich, führt allerdings zu einer Problematik bei kollektiven Daten. Diese wird in Abschnitt 4.2 basierend auf der in Abschnitt 4.1 vorgestellten Typisierung personenbezogener Daten diskutiert.

4.1 Typisierung von Daten

Bild 1 zeigt eine Typisierung von personenbezogenen Daten. Zunächst ist zu entscheiden, ob das betrachtete Datum für die vom Nutzer gewünschte und unmittelbar wahrnehmbare Zielfunktion erforderlich ist. Dementsprechend wird in funktional erforderliche und nicht-funktionale Daten unterschieden.

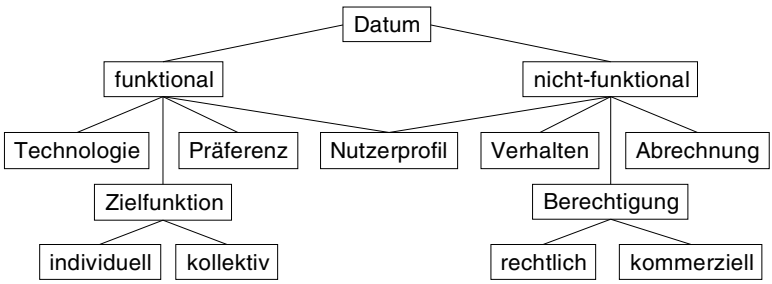

Bild 1 – Typisierung von personenbezogenen Daten

Funktionale Erforderlichkeit kann unterschiedliche Gründe haben. Zum einen kann die zur Realisierung verwendete Technologie das Datum erfordern wie z.B. IP Adressen im Internet. Des Weiteren kann die Zielfunktion selbst das Datum als Eingabewert benötigen. Zum Beispiel der aktuelle Aufenthaltsort für einen Dienst mit Ortsbezug. Nicht zuletzt kann die gewünschte Funktion durch Präferenzen parametrisiert werden, wie z.B. ob die Terminverwaltung anstehende Termine aktiv ankündigen soll.
Nicht-funktionale Daten werden für die eigentliche Erbringung der Zielfunktion nicht benötigt. Zu diesen zählt die Aufzeichnung des Nutzerverhaltens, um z.B. die Bedienungsfreundlichkeit einer Web-Anwendung bewerten und verbessern zu können. Des Weiteren sind Berechtigungen zu nicht-funktionalen Daten zu zählen, da diese vornehmlich zur Ausgrenzung von einzelnen Nutzern oder ganzen Nutzergruppen dienen. Dabei kann die Ausgrenzung entweder rechtlich oder kommerziell begründet sein. Zum Beispiel liegt eine rechtliche Ausgrenzung vor, wenn einem Nutzer ohne Führerschein das Mieten eines Autos verweigert wird. Nicht zuletzt sind Abrechnungsdaten als nicht-funktional einzustufen. Sie sind z.B. zur Bemessung des Dienstentgeldes und dessen Erhebung nötig.

Nutzerprofildaten entziehen sich einer eindeutigen und objektiven Zuordnung. Zum Beispiel ist eine funktionale Einordnung im Fall einer Buchempfehlung gemäß dem Schema „Kunden, die diesen Artikel gekauft haben, kauften auch …“ rechtfertigbar. Die gleichen Informationen lassen sich auch zu produktübergreifender Werbung nutzen. Etwa könnten nach Kauf eines Buches zum Thema „Computerbedienung“ verfügbare Computerkurse angeboten werden. Bereits in diesem Beispiel ist aus subjektiver Sicht zu klären, ob die Datenverwendung einer vom Nutzer gewünschten Funktion entspricht. Spätestens wenn die gleichen Nutzerprofildaten zu Zwecken wie z.B. Rasterfahndung genutzt werden, ist die Grenze zu nicht-funktionalen Daten überschritten.

4.2 Kollektive Daten und Grenzen der Technik

Die für die Zielfunktion erforderlichen Daten sind anhand des beschriebenen Personenkreises weiter zu unterscheiden. Falls ein Datum ein Individuum beschreibt, so ist dieses als individuell zu bezeichnen. Andererseits kann ein Datum eine Gruppe von Personen beschreiben, weshalb dieses als gemeinschaftlich aufzufassen ist. Digitale Soziale Netze beschreiben die sozialen Strukturen zwischen Nutzern und setzen damit stark auf die Verwendung kollektiver Daten. Kollektive Informationen sind nicht als Besitz eines Einzelnen zu verstehen. Vielmehr haben alle Individuen des betroffenen Personenkreises ein eigenständiges Interesse an und Recht auf Kontrollausübung bzgl. Erfassung, Verarbeitung, Speicherung und Weitergabe solcher Informationen.
Allein das mehrseitige Interesse einer Kontrollausübung stellt für existierende Zugriffskontrollmechanismen eine Herausforderung dar. Beim Zugriffskonzept Mandatory Access Control (MAC) [DoD85] steht die Kontrolle über Informationsflüsse aus Organisationssicht im Vordergrund. Zum Beispiel sollen Geschäftsgeheimnisse nur durch Vertrauensträger eingesehen werden können. Bei MAC ist jedem Datum eine Sensitivitätsstufe zugeordnet. Nutzer mit entsprechender Einstufung können zugreifen. Die Einstufung der Nutzer wird durch die Organisation vorgenommen und ist somit fremdbestimmt.
Im Gegensatz dazu legt bei Discretionary Access Control (DAC) [DoD85] der Nutzer, welcher die Information erfasst und/oder speichert, die Zugriffsrechte fest und behält die volle Kontrolle. Damit gibt es im DAC-Modell genau einen Besitzer von Daten, welcher zu jedem Zeitpunkt alleine über die Zugriffsberechtigungen bestimmt.
Schließlich fungiert beim Role Based Access Control (RBAC) [ANSI04] das Konzept der Rolle als Mittler zwischen Nutzer und Information. Eine Rolle kann hierbei als Handlungstypus interpretiert werden. Bei RBAC sind jeder Rolle Zugriffsrechte, jeder Information die notwendigen Zugriffsrechte und jedem Nutzer eine oder mehrere Rollen zugewiesen. Die verfügbaren Rollen und deren Zugriffsrechte sowie die Zuweisung von Rollen zu Nutzern erfolgt dabei durch den Systemadministrator der Organisation.
Allen Zugriffskontrollkonzepten gemein ist die Existenz einer allmächtigen Instanz – entweder in Form eines Systemadministrators oder eines Besitzers. Für die Anwendung in Sozialen Netzen sind diese Zugriffskontrollkonzepte somit nicht unmittelbar einsetzbar, denn für kollektive Informationen gibt es mehrere Interessen und somit Kontrollwünsche. Die Illusion der vollen Kontrollfähigkeit des Systems wird durch die technisch einfache Vervielfältigung von Information unterlaufen. Sobald Lesezugriff

gewährt wird, besteht das potenzielle Risiko der Vervielfältigung und damit der Existenz eines Duplikats ohne Zugriffsbeschränkung.
Hier könnte ein Umdenken hin zu kooperationsbasierten Ansätzen zu neuen Lösungswegen führen. Zum Beispiel betrachtet der Vorschlag Dual-Role Based Access Control (DRBAC) [GTK06] explizit zwei Domänen und deren Kooperation bei der Zugriffskontrolle im Umfeld des Grid Computing. Dennoch scheint die Gewährung des Rechts auf Vergabe von Zugriffsrechten und die Beschränkung der Weitergabe dieses Rechts bisher keine Beachtung zu finden. Letztlich folgt aus diesem Gedanken die Einführung von Kontrollmechanismen für die Verwaltung von Zugriffsrechten. Durch diese zusätzliche Kontrollstufe und Indirektion ist mit einer Zunahme der Komplexität der technischen Realisierung zu erwarten. Deshalb muss der potenzielle Mehrgewinn mit der größeren Komplexität und der Nutzbarkeit abgewogen werden.

5 Fazit

Die vorangehenden Ausführungen verdeutlichen, dass die Nutzung der IT für die Pflege sozialer Netzwerke und die Selbst(re)präsentation in einen Widerspruch zu dem Selbstbestimmungsanspruch von Individuen geraten kann. Eine durch die IT-Branche anvisierte Erhöhung der Autonomieansprüche des Einzelnen kann konterkariert werden, wenn (1) soziale Netzwerke die Offenlegung privater Daten quasi unerlässlich herausfordern: Individualisierung unterläuft unter diesen Umständen den Autonomiegedanken durch eine Aushöhlung des Datenschutzes. (2) Daten generell nicht eindeutig als persönliche abgegrenzt werden, wenn das Individuum in sozialen Netzwerken ein Knotenpunkt von Beziehungen ist. (3) Das Individuum in seinen Kompetenzen überfordert wird: der Selbstdatenschutz muss unter diesen Umständen paradoxerweise delegiert werden, häufig an Anbieter, die selber nicht transparent arbeiten oder einer öffentlichen Kontrolle unterliegen.

Literaturverzeichnis

[ANSI04] American National Standard for Information Technology, Role-based Access Control, ANSI INCITS 359-2004, 2004.

[DoD85] Department of Defense, Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Dezember 1985.

[GTK06] Ge, L., Tang S. und Kuang Q., Dual-Role Based Access Control Framework for Grid Services, Proceedings of the IEEE Asia-Pacific Conference on Services Computing, 2006.

[ISTAG01] ISTAG - Information Society Technologies Advisory Group der Europäischen Kommission (2001): Scenarios for Ambient Intelligence in 2010, ftp://ftp.cordis.europa.eu/pub/ist/docs/istagscenarios2010.pdf (Zugriff 24.4.2008).

[MIT04] MIT - Massachusetts Institute of Technology: Project Oxygen 2004, http://oxygen.lcs.mit.edu/ (Zugriff 24.4.2008).

[PH07] Pfitzmann, A. und Hansen, M. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Version 0.29, 2007.

[Ro06] Roßnagel, A. Datenschutz im 21. Jahrhundert. *Aus Politik und Zeitgeschichte. Beilage von: Das Parlament,* 5/06, http://www.bundestag.de/dasparlament/2006/05-06/beilage/002.html (Zugriff 24.4.2008)

[Rö01] Rössler, B.: Der Wert des Privaten. Frankfurt a. M. 2001.