REDE

Konrad-Adenauer-Stiftung e.V.

CHINA
KARSTEN WEBER

September 2007

www.kas.de/china
www.kas.de

Grundlagen der Informationsethik

VORTRAG ANLÄSSLICH DER INTERNATIONALEN KONFERENZ "ETHIK INTERDISZIPLINÄR: WIRTSCHAFTSETHIK, WISSENSCHAFTSETHIK, TECHNIKETHIK"

Es ist fast schon trivial zu sagen, dass Informations- und Kommunikationstechnologie (IuK) beinahe alle Bereiche des Lebens durchdringt. Zwar gilt dies beileibe noch nicht für alle Menschen der Welt, doch in den entwickelten Ländern ebenso wie in vielen der sich entwickelnden Ländern kommen immer mehr Menschen im Informationszeitalter an.

Das gilt insbesondere für Asien und hier für China und Indien. Beide Länder zeigen eine rasante Entwicklung auf technischem und wirtschaftlichem Gebiet. Dies führt dazu, dass immer mehr Menschen sowohl am Arbeitsplatz als auch in ihrem privaten Leben mit IuK-Technologie konfrontiert werden und mit dieser umzugehen lernen müssen.

Die Nutzung von IuK-Technologie eröffnet viele Chancen und kann einen hohen gesellschaftlichen wie individuellen Nutzen produzieren. Gleichzeitig existieren Risiken und Schadenspotenziale, wiederum sowohl auf der gesellschaftlichen als auch auf der individuellen Ebene.

Damit Chancen realisiert und Risiken vermieden werden können und so ein nützlicher Umgang mit IuK-Technologie erreicht werden kann, bedarf es Regeln. Wie in allen anderen Lebensbereichen auch müssen Rechte und Pflichten sowie Verantwortlichkeit für den Umgang mit IuK-Technologie klar definiert werden. In modernen Staaten geschieht dies vor allem im Bereich der Rechtssetzung und Rechtsprechung: Der politische Souverän entwickelt und verabschiedet Gesetze, die in einer unabhängigen Gerichtsbarkeit durchgesetzt werden. Solche Gesetze benötigen jedoch eine Legitimationsbasis, die bspw. aus den geteilten moralischen Überzeugungen der Bürger eines Landes bestehen kann. Hierin unterscheidet sich Informationsethik nicht von anderen Ethiken.

Unglücklicherweise wird jener Zweig der angewandten Ethik, der sich mit IuK-Technologie beschäftigt, nicht einheitlich benannt. Im Folgenden soll zwar immer von Informationsethik gesprochen werden, doch sehr weit verbreitet ist auch die Bezeichnung Computerethik (engl.: computer ethics, bspw. Johnson 2001), oft findet sich Cyberethik (engl.: cyber ethics, bspw. Spinello 2003) oder, meist nur im Deutschen, Netzethik oder Internetethik (bspw. Hausmanninger, Capurro 2002), in neueren Texten, wiederum insbesondere in deutschsprachigen Publikationen, wird von Informationsethik (engl.: information ethics, bspw. Spinner, Nagenborg, Weber 2001) gesprochen.

Noch vielfältiger als die Bezeichnungen sind die Themen, mit denen sich Informationsethik auseinandersetzt, bspw. digitale Spaltung (engl.: digital divide) und soziale Teilhabe durch IuK-Technologie, elektronische Demokratie (engl.: e-democracy) und „Empowerment“ von Menschen durch IuK-Technologie, Urheberrechtsfragen (engl.: copyright) und die Diskussion um den freien Informationszugang (engl.: open access), der Schutz der Privatsphäre (engl.: privacy), Datenschutz und dazu entgegengesetzt Überwachung (engl.: surveillance) und Kon-

Konrad Adenauer Stiftung

Konrad-Adenauer-Stiftung e.V.

CHINA
KARSTEN WEBER

September 2007

www.kas.de/china
www.kas.de

trolle, die Veränderungen persönlicher und gesellschaftlicher Beziehungen sowie das Problem der technischen Modifikation und der Erweiterung (engl.: enhancement) des menschlichen Körpers durch IuK-Technologie. Nicht alle genannten Problemfelder liegen im Kern der Informationsethik, für manche Fragen entwickeln sich derzeit neue angewandte Ethiken, bspw. zur Frage von Computer- und Roboterrechten.

1. HISTORISCHE ENTWICKLUNG

Sehr wichtig hingegen und historisch gesehen auch Ausgangspunkt der Informationsethik ist die Frage nach dem moralisch und gesellschaftlich richtigen Umgang mit Informationen, insbesondere personenbezogenen Informationen, mit deren Hilfe man Menschen überwachen, kontrollieren und beeinflussen könnte. Dies zeigt bereits ein Blick in die Entwicklung der Informationsethik. Obwohl es eine geraume Zeit dauerte, bis Bezeichnungen wie „Informationsethik“ allgemein gebräuchlich wurden, liegt die Geburtsstunde des Themenfeldes und der damit beschäftigten angewandten Ethik recht weit zurück – zumindest, wenn man bedenkt, wie kurz die Zeit ist, seitdem Computer überhaupt existieren.

Aus einer historischen Perspektive ist der betrachtete Zeitraum recht kurz, umfasst er doch selbst bei großzügiger Auslegung kaum mehr als 60 Jahre. Einige der aktuellen und konkreten Themenfelder wurden oben bereits angedeutet; in der Literatur werden Problembereiche etwas abstrakter zusammengefasst mit „property, access, privacy, and accuracy“ (Britz 1999: 25), abgekürzt mit dem Akronym PAPA. Diese Festlegung stammt aus einer Zeit, als bspw. das Internet in der Öffentlichkeit noch kaum eine Rolle spielte oder das Problem der Eigentumsverletzung durch IuK-Technologie außerhalb spezifischer Fachdiskussionen unbekannt war. Richard O. Mason (1986) nannte diese Themen bereits in den 1980er Jahren (vgl. Eining, Lee 1997). Allerdings wurde schon in den 1970er Jahren intensiv über Privatsphäre und Datenschutz diskutiert und in diesem Zusammenhang zumindest „privacy“ und „accuracy“ thematisiert (vgl. Hoffman 1973; Martin 1973). Tatsächlich muss noch ein paar Jahre weiter zurückgegangen werden, um wichtige Ursprünge der Informationsethik aufzuzeigen, die wiederum mit dem Schutz der Privatsphäre bzw. mit Datenschutz auf der einen Seite und technisierter Überwachung auf der anderen Seite zusammenhängen. Alan F. Westin publizierte bereits 1967 sein nach wie vor oft zitiertes Buch „Privacy and Freedom“. Es ist stilbildend für die gesamte nachfolgende Diskussion, weil hier bereits der Zusammenhang zwischen dem Schutz der Privatsphäre und Freiheit im Allgemeinen hergestellt und betont wird. In Deutschland bspw. etablierte sich das Thema des Datenschutzes spätestens mit dem so genannten „Volkszählungsurteil“ des Bundesverfassungsgerichts vom 15.12.1983 (BVG 1983). Das Gericht stellte fest, dass IuK-Technologie starken Einfluss auf die Wahrung persönlicher verfassungsmäßig garantierter Rechte haben kann und dass bereits existierende Grundgesetzartikel gegen die technisch realisierten Möglichkeiten der Verarbeitung personenbezogener Daten Schutz böten und ein so genanntes „informationelles Selbstbestimmungsrecht“ konstituierten.

Gleichzeitig wird aber formuliert, dass dieser Schutz dort ende, wo ein „überwiegendes Allgemeininteresse“ vorliege – auf diesen Konflikt zwischen individuellen Rechten und Allgemeinwohl geht bspw. Amitai Etzioni (1999) ein, wenn er dafür plädiert, Privatsphäre zugunsten des Allgemeinwohls einzuschränken. Die Gefahr des Rekurses auf das Allgemeinwohl liegt jedoch darin, dass dieser Ausdruck schwer zu definieren ist und damit fast beliebige Eingriffe in individuelle Rechte begründet werden können – es bedarf also expliziter Aussagen darüber, was zum Allgemeinwohl gehört und wo es durch individuelle Rechte Grenzen findet.

1.1. Definitionen

Da der Schutz der Privatsphäre in der Informationsethik eine dominante Stellung einnimmt, soll im Folgenden vor allem hierauf eingegangen werden. Der englische Ausdruck „privacy“ wurde durch den Artikel „The Right to Privacy“ von Samuel D. War-

Konrad-Adenauer-Stiftung e.V.

CHINA
KARSTEN WEBER

September 2007

www.kas.de/china
www.kas.de

ren und Louis D. Brandeis aus dem Jahr 1890 geprägt. Privatsphäre bedeutet dort „the right to be let alone“: das Recht, in Ruhe gelassen und nicht gestört zu werden. Diese Formel selbst verrät aber noch nicht, wobei und bis zu welchem Grad dieses Recht wirkt; es gilt also, genauer zu bestimmen, worin dieses Recht, allein gelassen zu werden, besteht. Allerdings hinterlässt ein Blick in die Literatur eher Verwirrung, als dass er klärend wirkt, denn allgemein akzeptierte Definitionen, Theorien und Wirkungsbereiche wird man schwerlich finden. Gary Marx (2001: 161) bringt diese Situation recht lakonisch auf den Punkt:

„[…] the mental cacophony associated with the rich variety of empirical configurations seen with electronic surveillance and other forms of information technology stems from the failure to differentiate between, and note the inter-relations of various dimensions of the public and private.“

Mit diesem Zitat trägt Marx noch zur Unklarheit bei, denn das Private scheint durch ein Anderes mitdefiniert zu sein: das Öffentliche oder die Öffentlichkeit. Dabei, so Diane Michelfelder (2001: 129), dürfen wir aber nicht von unserem Alltagsverständnis ausgehen:

„When philosophers with an interest in privacy move beyond discussing its commonsense meaning to a consideration of more complex issues, […], they quickly find themselves in a terrain characterized by a lack of clear agreement over a variety of fundamental aspects of privacy, including its scope, definition, and value.“

Wenn man die Theoriebildung im Bereich der Privatsphäre betrachtet, wird man eine Vielzahl von Ansätzen finden; Herman Tavani (1999) bspw. hat versucht, hierfür eine systematische Klassifikation vorzulegen.[1] Daneben hat Beate Rössler (2001) einen vielbeachteten Entwurf entwickelt, um Privatsphäre – oder Privatheit, wie sie sagt – begrifflich zu fassen und ethisch zu evaluieren. Obwohl dieser Ansatz durchaus systematische Schwierigkeiten mit sich bringt, bietet er theoretische Werkzeuge, um mehr Klarheit in die Diskussion um Privatsphäre zu bringen. Rössler unterscheidet drei Dimensionen: dezisionale, informationelle und lokale Privatheit (ibid.: 144ff.). Bei der dezisionalen Dimension geht es darum, dass Entscheidungen sowie „Handlungen, Verhaltensweisen und Lebensweisen“ (ibid.: 145) einer Person nicht nur selbst bestimmt und gewählt werden, sondern auch darum, das Dritte sich der Bewertung, jedes Einspruch, Kommentars oder Urteils darüber enthalten müssen. Als Beispiel können die religiösen Ansichten von Personen genant werden. Wird dezisionale Privatheit gewährt, sollen diese den Menschen in einer Gesellschaft selbst überlassen bleiben und nicht durch irgendwelche Instanzen, seien sie staatlicher oder hier insbesondere religiöser Natur, vorgeschrieben und erzwungen werden.[2] Die informationelle Dimension der Privatheit impliziert, dass Personen kontrollieren können, wer welche Informationen über die eigene Person und die eigenen Lebensumstände erhält. Hierzu finden sich eigenständige Theorien, die oft als „control theories of privacy“ (bspw. Spinello 2003: 143) bezeichnet werden. Doch oft wissen Menschen gar nicht, wo und von wem Informationen über ihre Handlungen gesammelt werden, obwohl dies massenhaft geschieht (Stalder 2002: 120):

„The creation, collection and processing of personal data is nearly a ubiquitous phenomenon. Every time we use a loyalty card at a retailer, our names are correlated with our purchases and entered into giant databases. Every time we pass an electronic toll booth on the highway, every time we use a cell phone or a credit card, our locations are being recorded, analyzed and stored. Every time we go to see a doctor, submit an insurance claim, pay our utility bills, interact with the government, or go online, the picture gleaned from our actions and states grows finer and fatter.“

Wir verfügen dabei kaum mehr über die Kontrolle über personenbezogene Daten – und dies kann sich auf unsere Freiheit auswirken (BVG 1983):

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen

Konrad-Adenauer-Stiftung e.V.

CHINA
KARSTEN WEBER

September 2007

www.kas.de/china
www.kas.de

in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."

Durch das Internet und darauf aufbauende Kommunikationsformen bekommt das damit angesprochene Problem eine neue Dimension, wie Barrera und Okai (1999: 1) lapidar bemerken:

„To be in cyberspace is to be recorded. Digital activities and objects are nothing but an ensemble of traces and records. Each electronic action in cyberspace implies the creation of tread marks […]. Those digital footprints can be, by nature, reconstituted, recreated and saved indefinitely."

Es ist also beileibe nicht immer klar, ob wir informationelle Privatheit herstellen können, da ihre Wahrung oder Gefährdung unter anderem mit dem gesellschaftlichen Umgang mit physisch definierten Räumen einhergeht. Dies nimmt die lokale Dimension der Privaheit auf (Rössler 2001: 255ff.): Die „eigenen vier Wände" stellen das wichtigste Refugium dar, das der Überwachung explizit entzogen sein soll. Hier ist dezisionale und informationelle Privatheit gleichsam natürlich gegeben; weder erfahren Dritte etwas über das eigene Handeln, noch haben sie die Möglichkeit, ihren Einspruch zu erheben – sowohl die Informationen über das eigene Handeln als auch die Urteile und Bewertungen „prallen" von den eigenen vier Wänden ab.[3]

Aus Sicht einer liberal geprägten Informationsethik ist die Sicherung von dezisionaler, informationeller und lokaler Privatheit essentiell sowohl für das individuelle Leben als auch für das gesellschaftliche Wohl. Nur dann, wenn diese Formen der Privatheit gegeben sind, können sich Menschen zu selbstbewussten, kritischen und kreativen, leistungsfähigen und leistungswilligen Personen entwickeln, die einen Beitrag zum gesellschaftlichen Fortschritt leisten können. Folgt man dieser Sicht, ist die Herstellung und Wahrung von Privatheit eine der wichtigsten Aufgaben eines jeden Staates, unabhängig von der Regierungsform.

Hieraus erwächst ein Problem, da die eigenen vier Wände lange Zeit dazu missbraucht wurden, Übergriffe auf andere Personen, insbesondere von Frauen und Kindern, den Blicken der Öffentlichkeit und deren Sanktionsmöglichkeiten zu entziehen, bspw. bei ehelicher Gewalt. Dies führte in der feministischen Debatte zur Prägung des Schlagworts, dass das Private öffentlich bzw. politisch sei (vgl. Pateman 1992: 456), da dort Handlungen vollzogen würden, die in Rechte von Personen eingriffen und deshalb der öffentlichen Bewertung und gegebenenfalls Sanktionierung nicht entzogen werden dürften (s. a. DeCew 1997: 81ff.).

1.2. Privatsphäre und Überwachung

Das bisher Gesagte darf allerdings nicht so verstanden werden, dass Privatsphäre einen physischen Raum, im Fall der lokalen Dimension, oder einen sozialen Raum, im Fall der dezisionalen und informationellen Dimension der Privatheit, herstellte, der jeglicher Kontrolle entzogen wäre. Die eigenen vier Wände bewohnen wir, ob temporär oder dauerhaft, meist nicht allein. Außerdem existieren Kommunikationswege nach außen – hoch technisiert in Form von Telefon oder Internet, einfacher in Form von Fenstern und Türen. Völlige Abschottung durch Kappung aller Kommunikationsmöglichkeiten und Ausschluss anderer Personen bedeutete Isolation und diese wiederum widerspräche elementaren Bedürfnissen des sozialen Wesens Mensch. In dem Augenblick aber, wo Menschen Kommunikation zulassen, besteht immer auch die Möglichkeit und die Notwendigkeit von Kontrolle und Überwachung. Beide sind nicht abhängig von der Existenz und Nutzung von IuK-Technologie, sondern gehören zu den sozialen Notwendigkeiten im Zusammenleben von Menschen. Kontrolle und Überwachung finden im Stammesverband statt, in der Gesangsgruppe, im Fußballverein, am Arbeitsplatz, in der Dorfgemeinschaft, kurz: Überall, wo Menschen miteinander leben oder interagieren. All diese sozialen Zusammenhänge unterscheiden sich nicht darin, ob Kontrolle und Überwachung stattfinden,

sondern nur, in welchem Ausmaß dies geschieht. Wenn man Michel Foucault (1975) folgt, ist der paradigmatische Ort in dieser Hinsicht das Gefängnis. In seiner idealen Form, dem Bentham'schen Panopticon (vgl. Elden 2003), führt die bloße Möglichkeit der Überwachung dazu, dass sich die Gefangenen durch Selbstkontrolle selbst disziplinieren.

Foucault und nach ihm viele andere Autoren (vgl. die Beiträge in Lyon 2006) haben dieses Konzept auf moderne Gesellschaften angewendet: Die Idee ist, dass solche Gesellschaften nur dadurch existieren können, dass sich die Bürger stetig selbst überwachen und kontrollieren und dadurch disziplinieren (vgl. Vaz, Bruno 2003). Sie handeln entsprechend der internalisierten Erwartungen an sie. Dies drückt sich auch im schon genannten Volkszählungsurteil aus: Überwachung oder der bloße Eindruck, überwacht zu werden, kann dazu führen, dass Menschen ihr Verhalten in Richtung eines tatsächlichen oder vorgestellten Konformitätsdrucks verändern – dies aber widerspricht der Vorstellung einer liberalen Gesellschaft. Hier gilt, dass Überwachung und Kontrolle auf das notwendige Minimum reduziert bleiben muss.

Dies kann zwar variieren, bspw. in Krisenzeiten, aber der Grad von Überwachung und Kontrolle sollte stetig durch den politischen Souverän minimal gehalten werden.

Obwohl Überwachung und Kontrolle zwar in einem gegensätzlichen, aber doch engen Zusammenhang zu Privatsphäre stehen und daher aus theoretischer wie praktischer Sicht gemeinsam behandelt werden müssten, entstand in den letzten Jahren eine Diskussion um theoretische Zugänge, die nicht mehr nur auf das Wechselspiel von Privatsphäre auf der einen und Kontrolle und Überwachung auf der anderen Seite abheben, sondern auf die soziale Funktion von Kontrolle und Überwachung fokussieren, wobei IuK-Technologie eine wichtige Rolle spielt. „Surveillance studies" thematisieren dabei zunehmend, wie sich der öffentliche Raum durch Überwachung verändert (bspw. Koskela 2000 & 2003; s. a. die Beiträge in Lyon 2003).

Foucault bezog seine Ideen nicht in erster Linie auf die eigenen vier Wände, sondern auf Straßen und Plätze, Büros, Einkaufsmeilen oder auch Kneipen, Kirchen, Museen, kurz: auf die allgemein oder doch zumindest für viele Menschen zugänglichen Räume, die wir alltäglich aufsuchen (müssen). Aus einer informationsethischen Sicht ist nun bspw. zu fragen, welcher moralische und/oder soziale Wert damit verbunden ist, im öffentlichen Raum nicht ständig der Kontrolle und Überwachung unterworfen zu sein (bspw. Nissenbaum 1998; Patton 2000), welchen moralischen und/oder sozialen Stellenwert Sicherheit hat, wie die Konflikte zwischen Nichtüberwachung und Sicherheit austariert werden könnten – wiederum wird hieran deutlich, dass Informationsethik nicht isoliert von rechtlichen, politischen, sozialen oder ökonomischen Aspekten betrieben werden kann (sehr deutlich in Graham, Wood 2003).

1.3. Pessimistische Sichten

„You already have zero privacy – get over it" (zitiert in Marfkoff 1999): Dieses Zitat von Scott McNealy, dem damaligen CEO von Sun Microsystems, erregte große Aufmerksamkeit; zum Ende des 20. Jahrhunderts markierte es eine sehr pessimistische Sicht auf Privatsphäre. Damit stand und steht McNealy jedoch nicht allein, wobei sich der Pessimismus auf verschiedene Weise ausdrücken kann. David Brin veröffentlichte 1998 sein Buch „The Transparent Society", in dem er die Rechnung aufmacht, dass wir, um unsere liberale Gesellschaft zu erhalten, Privatsphäre und Datenschutz opfern müssten, da nur Wissen uns befähigen würde, eine freiheitliche Gesellschaft gegen Bedrohungen durch Regierungen, Unternehmen und uns selbst zu schützen. Wichtig ist für Brin „accountability" – die Zurechenbarkeit von Handlungen und deren Folgen zu Personen, Gruppen, Unternehmen oder Institutionen. Zurechenbarkeit ist aber nur durch Information möglich – daher sieht er einen Widerspruch zwischen Privatsphäre und Freiheit. Ähnlich pessimistisch argumentiert Reg Whitaker (1999), allerdings ohne Brins optimistische Wendung zur Freiheit. Etwas später prognostizierte Simson Garfinkel (2000) den Tod der Privatsphäre in 21.

Jahrhundert. Allerdings argumentiert er, dass Privatsphäre zwar erheblich bedroht sei, aber verteidigt werden müsse, da sie Basis jeder Freiheit und des Lebens sei. Garfinkel folgt hier letztlich einer Argumentation, die sich bereits bei John Stuart Mill in On Liberty aus dem Jahr 1859 findet: bestimmte Freiheiten, zu der die Privatsphäre zählt, sind notwendig, damit sich Menschen zu kreativen Personen entwickeln können, die durch die Wahl eigener Lebensentwürfe neue Lösungen für gesellschaftliche Probleme entwickeln und so zum Allgemeinwohl beitragen. Generell kann man formulieren, dass in der Literatur zur Informationsethik ein skeptischer Grundton überwiegt, bspw. in Hinblick auf die Einflussmöglichkeiten von Ethik auf Politik, Recht und Wirtschaft, dass aber gleichzeitig die Versuche überwiegen, konstruktive Beiträge zur Lösung entsprechender Probleme zu liefern – Brins und Whitakers generell pessimistische Sichtweisen sind daher als Ausnahmen zu sehen.

2. WOHIN DIE REISE GEHEN WIRD

Tatsächlich gibt es gute Gründe zur Sorge, bspw. in Hinblick auf Biometrie und ihren Einfluss auf Privatsphäre oder die Gestaltung des öffentlichen Raums. Es ist jedoch nicht so sehr die Technologie selbst, von der diese Gefahr ausgeht, sondern die Denkweisen, die ihrem Einsatz vorangehen (vgl. Weber 2006a & 2006b). Zurzeit lässt sich in verschiedenen Bereichen feststellen, dass viele Menschen bereit sind, ganz oder teilweise auf Datenschutz und Privatsphäre zu verzichten, wenn sie dafür aus subjektiver Sicht in den Genuss von Vorteilen kommen; darauf basieren bspw. die schon länger bekannten Rabattkartensysteme.

Sollen solche und ähnliche Konflikte im Rahmen der Informationsethik nicht nur nachholend beschrieben und beklagt, sondern aktiv Einfluss auf die Entwicklung und Implementierung von IuK-Technologie genommen werden, wird es in Zukunft notwendig sein, bestimmten Sichtweisen der Informationsethik nicht weiter zu folgen. Informationsethik ist keine Berufsethik jener Menschen, die professionell mit Informationen arbeiten – schon allein deshalb, weil es faktisch unmöglich ist, hier eine sinnvolle Abgrenzung vorzunehmen. Informationsethik darf aber auch nicht als Tugendethik betrieben werden. Ohne Zweifel sind individuelle Tugenden für moralisches Handeln wichtig, aber zum einen sind sie in Zeiten pluralistischer Gesellschaften – plural bspw. in Hinblick auf ethnische Herkunft, weltanschauliche und religiöse Überzeugungen, Lebensentwürfe – nicht universalisierbar und zum anderen ist die Reichweite von Tugenden begrenzt – sie reicht kaum weiter als zu Verwandten, Freunden, Arbeitskollegen und Vereinsmitgliedern: Tugenden taugen für den Nahbereich, aber nicht für eine globalisierte Welt. Die oben genannten Beispiele zeigen bereits, dass Informationsethik davon handeln muss, wie kollidierende Rechte und Freiheiten austariert werden können. Daher ist es eine notwendige Schlussfolgerung, dass sich Informationsethik auf das Fundament der Sozial- und politischen Philosophie stützen sollte (ausführlich Weber 2005). Deshalb muss Informationsethik in gewisser Weise von Moral Abschied nehmen: Insoweit nämlich, dass es – wie Ethik oft missverstanden wird – nicht um individuelle Moral geht, sondern um die Gestaltung gesellschaftlich verbindlicher Regeln für den Umgang mit Informationen: Man kann bspw. für ein uneingeschränktes Recht auf freie Meinungsäußerung eintreten und trotzdem im individuellen Handeln aus moralischen Gründen nicht alles aussprechen. Es geht in der Informationsethik also um einen „overlapping consensus“, wie es John Rawls (1987) ausdrückte, den Bürger einer Gesellschaft teilen, ohne in ihren moralischen Überzeugungen auf diesen reduziert zu sein. Die Bedingung der Möglichkeit eines Konsenses aber ist der freie Informationsaustausch in einer Gesellschaft – neben der Wahrung von Privatsphäre wohl eines der drängendsten Probleme moderner Gesellschaften.[4]

3. ÜBER DEN AUTOR

Dr. phil. habil. Karsten Weber

- Professor für Philosophie an der Universität Opole, Polen
- Honorarprofessor für Kultur und Technik an der Brandenburgischen

Konrad-Adenauer-Stiftung e.V.

CHINA
KARSTEN WEBER

September 2007

www.kas.de/china
www.kas.de

Technischen Universität Cottbus, Deutschland

- Privatdozent für Philosophie an der Europa-Universität Viadrina Frankfurt (Oder), Deutschland

- E-Mail: kweber@euv-frankfurt-o.de

4. LITERATUR

Barrera, M. H.; Okai, J. M. (1999): Digital Correspondence: Recreating Privacy Paradigms, in: International Journal of Communications Law and Policy 3, (<http://www.ijclp.org/3_1999/pdf/ijclp_webdoc_4_3_1999.pdf>, zuletzt besucht am 28.08.2007).

Brin, D. (1998): The Transparent Society. Reading/Massachusetts: Perseus Books.

Britz, J. J. (1999): Access to Information: Ethical Guidelines for Meeting the Challenges of the Information Age, in: Pourciau, L. J. (ed.): Ethics and Electronic Information in the Twenty-First Century. West Lafayette/Indiana: Purdue University Press, S. 9-28.

BVG (1983): Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15.12.1983 auf die mündliche Verhandlung vom 18. und 19.10.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden (<http://www.datenschutzberlin.de/gesetze/sonstige/volksz.htm>, zuletzt besucht am 27.07.2007).

DeCew, J. W. (1997): In Pursuit of Privacy. Law, Ethics, and the Rise of Technology. Ithaca, London: Cornell University Press.

Eining, M. M.; Lee, G. M. (1997): Information ethics: An exploratory study from an international perspective, in: Journal of Information Systems 11 (1), S. 1-17.

Elden, St. (2003): Plague, Panopticon, Police, in: Surveillance & Society 1 (3), S. 240-253 (<http://www.surveillance-and-society.org/articles1(3)/ppp.pdf>, zuletzt besucht am 31.07.2007).

Etzioni, A. (1999): The Limits of Privacy. New York: Basic Books.

Foucault, M. (1975): Surveiller et punir. La naissance de la prison. Paris: Editions Gallimard.

Garfinkel, S. (2000): Database Nation. Sebastopol/California: O'Reilly.

Graham, St.; Wood, D. (2003): Digitizing Surveillance: Categorization, Space, Inequality, in: Critical Social Policy 23(2), S. 227-248.

Hausmanninger, Th.; Capurro, R. (2002, Hrsg.): Netzethik. Grundlegungsfragen der Internetethik. München: Fink.

Hoffman, L. J. (1973): Security and privacy in computer systems. Los Angeles: Melville Publications.

Johnson, D. (32001): Computer Ethics. Upper Saddle River/New Jersey: Prentice Hall.

Koskela, H. (2000): 'The gaze without eyes': video-surveillance and the changing nature of urban space, in: Progress in Human Geography 24 (2), S. 243-265.

Koskela, H. (2003): 'Cam Era' – the contemporary urban Panopticon, in: Surveillance & Society 1 (3), S. 292-313 (<http://www.surveillance-and-society.org/articles1(3)/camera.pdf>, zuletzt besucht am 31.07.2007).

Lyon, D. (2003, ed.): Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination. London, New York: Routledge.

Lyon, D. (2006, ed.): Theorizing Surveillance. The panopticon and beyond. Portland/Oregon: Willian Publishing.

Marfkoff, J. (1999): Growing Compatibility Issue: Computers and User Privacy, in: The New York Times, Ausgabe vom 03. März, S. A1.

Martin, J. (1973): Security, accuracy, and privacy in computer systems. Englewood Cliffs/New Jersey: Prentice Hall.

Marx, G. T. (2001): Murky conceptual waters: The public and the private, in: Ethics and Information Technology 3, S. 157-169.

Mason, R. O. (1986): Four ethical issues of the information age, in: MIS Quarterly 10 (1), S. 4-12.

Michelfelder, D. P. (2001): The moral value of informational privacy in cyberspace, in: Ethics and Information Technology 3, S. 129-135.

Nagenborg. M. (2005): Das Private unter den Rahmenbedingungen der IuK-Technologie. Ein Beitrag zur Informationsethik. Wiesbaden: VS Verlag für Sozialwissenschaften.

Nissenbaum, H. (1998): Protecting Privacy in an Information Age: The Problem of Privacy in Public, in: Law and Philosophy 17, S. 559-596.

Pateman, C. (1992): Feminist Critiques of the Public/Private Dichotomy, in: Kymlicka, W. (ed.): Justice in Political Philosophy, Volume II. Aldershot: Edward Elgar Publishing, S. 234-296 (Erstveröffentlichung in: Phillips, A. (1981, ed.): Feminism and Equality. Oxford: Blackwell).

Patton, J. W. (2000): Protecting privacy in public? Surveillance technologies and the value of public places, in: Ethics and Information Technology 2, S. 181-187.

Rawls, J. (1987): The Idea of an Overlapping Consensus, in: Oxford Journal of Legal Studies 7 (1), S. 1-25.

Rössler, B. (2001): Der Wert des Privaten. Frankfurt/Main: Suhrkamp.

Spinello, R. A. (22003): Cyber Ethics. Morality and Law in Cyberspace. Sudbury/Massachusetts: Sudbury.

Spinner, H.; Nagenborg, M.; Weber, K. (2001): Bausteine zu einer neuen Informationsethik. Berlin, Wien: Philo.

Stalder, F. (2002): Opinion. Privacy is not the antidote to surveillance, in: Surveillance & Society 1 (1), S. 120-124 (<http://www.surveillance-and-society.org/articles1/opinion.pdf>, zuletzt besucht am 31.07.2007).

Tavani, H. T. (1999): KDD, data mining, and the challenge for normative privacy, in: Ethics and Information Technology 1, S. 265-273.

Vaz, P.; Bruno, F. (2003): Types of Self-Surveillance: from abnormality to individuals 'at risk', in: Surveillance & Society 1 (3), S. 272-291 (<http://www.surveillance-andsociety. org/articles1(3)/self.pdf>, zuletzt besucht am 31.07.2007).

Warren, S. D.; Brandeis, L. D. (1890): The Right to Privacy, in: Harvard Law Review, IV (5), S. 193ff.

Weber, K. (2005): Das Recht auf Informationszugang. Berlin: Frank & Timme.

Weber, K. (2006b): The Next Step: Privacy Invasions by Biometrics and ICT Implants, in: Ubiquity. An ACM IT Magazine and Forum 7 (45), (<http://www.acm.org/ubiquity/views/pf/v7i45_weber.pdf>, zuletzt besucht am 31.07.2007).

Weber, K. (2006b): Privacy invasions, in: EMBO Reports, Science and Society, Special Issue "Science and Security" 7, S. S36-S39.

Westin, A. F. (1967): Privacy and Freedom. New York: Atheneum.

Whitaker, R. (1999): The End of Privacy. New York: The New Press.

Anmerkungen

[1] Nagenborg (2005: 18ff.) bietet sowohl einen guten Überblick als auch konstruktive Kritik.

[2] Solche Präferenzen müssen selbstverständlich unter dem Vorbehalt stehen, dass nicht die Rechte anderer Personen verletzt werden. So müssen die unmittelbar Beteiligten zustimmungsfähig und -willig sein, auf sie darf kein Zwang ausgeübt werden. Reli-

giöse Bräuche dürfen also keinen Missbrauch anderer Menschen oder Verbrechen implizieren.

[3] Hieraus erwächst ein Problem, da die eigenen vier Wände lange Zeit dazu missbraucht wurden, Übergriffe auf andere Personen, insbesondere von Frauen und Kindern, den Blicken der Öffentlichkeit und deren Sanktionsmöglichkeiten zu entziehen, bspw. bei ehelicher Gewalt. Dies führte in der feministischen Debatte zur Prägung des Schlagworts, dass das Private öffentlich bzw. politisch sei (vgl. Pateman 1992: 456), da dort Handlungen vollzogen würden, die in Rechte von Personen eingriffen und deshalb der öffentlichen Bewertung und gegebenenfalls Sanktionierung nicht entzogen werden dürften (s. a. DeCew 1997: 81ff.).

[4] Damit ist das zweite wichtige Thema der Informationsethik angesprochen, das hier aber nur genannt und nicht mehr ausführlich diskutiert werden kann, ebenso wie das Thema der Urheberrechte. Informationsfreiheit, Privatsphäre, Urheberrechte: Die Ansprüche, die mit diesen drei Problemfeldern verbunden sind, stehen wechselseitig in einem Konkurrenzverhältnis, stützen sich aber auch teilweise. Deshalb können sie im Grunde nicht isoliert diskutiert werden – der vorliegende Text ist in dieser Hinsicht also notwendiger Weise unvollständig.