

„Digitaler Ethik“ die Rede (Grimm/Keber/Zöllner 2019; Spiekermann 2019; Capurro 2009), seltener von ‚Datenethik‘ oder (unspezifischer) von der ‚Ethik des digitalen Zeitalters‘. Das wichtigste unter den zahlreichen neuen Schwerpunktthemen innerhalb dieses Bereichs ist vielleicht die Ethik der Algorithmen/Algorithmenethik (Hustedt 2019). Daneben gibt es etwa die Ethik der Künstlichen Intelligenz, die Roboterethik und die Ethik der Mensch-Maschine-Interaktion. Ältere Bereichsethiken wie die vom Ansatz her umfassendere Informationsethik und die Computerethik sind im Wesentlichen in diesen neuen Ansätzen aufgegangen. Auch der Begriff ‚Cyberethik‘ (Kolb et al. 1998; Frohmann 2002) ist weniger verbreitet. ‚Netzethik‘ bezieht sich spezieller auf Fragen, die das Internet betreffen (Hausmanninger/Capurro 2002). Der Begriff ‚Hackerethik‘ bezeichnet die moralischen Richtlinien, die sich die Hackerszene gegeben hat, und die auf dem Prinzip aufbauen, dass alle Information frei zugänglich sein sollte (Himanen 2001; www.hacker-ethik.de). ‚Eper-Ethik‘ steht für Überlegungen, ob der Umgang mit intelligenten Softwareagenten, sogenannten elektronischen Personen oder *epers* (*electronic personas*), einer eigenen Ethik bedarf. Alle diese Bereiche haben zahlreiche Berührungspunkte mit anderen Bereichsethiken, vor allem mit der Technik- und der Medienethik. Im Bereich des Einsatzes dieser Technologien in der Medizin gibt es Berührungspunkte mit der Medizinethik, wenn es um Fragen der Zuschreibung von Verantwortung geht, mit der Rechtsethik und auch mit der politischen Philosophie (Weber 2001; 2002). Ebenso relevant sind Disziplinen wie die Psychologie und, bei Fragen nach der kulturspezifischen Gestaltung der digitalen Technologie, auch die Ethnologie.

‚Netiquette‘ hingegen ist kein originär moralischer Ansatz, sondern umfasst Regeln für das gute Benehmen im Netz, die von Community zu Community sehr unterschiedlich gehandhabt, von manchen Autoren aber als erster Schritt auf dem Weg zu einer Internetethik verstanden werden (Greis 2002; Hammwöhner/Wolff 2009).

Während das Ziel der Digitalen Ethik darin besteht, eine umfassende Reflektion und

Grundlegung einer Ethik unter den Bedingungen der Digitalisierung zu formulieren, befassen sich die Teilbereiche mit zum Teil sehr stark spezialisierten Fragestellungen. Da sich sowohl die Technik als auch die philosophisch-ethische Reflexion über ihre Verwendung derzeit rasant wandeln, ist dieser Bereich nicht abschließend zu systematisieren. Welche der aktuellen Themenfelder als eigene Bereichsethiken gefasst werden sollten, ist offen. Viele Vertreter der Digitalen Ethik sehen ihre Aufgabe auch darin, zur Verbreitung von digitaler Kompetenz beizutragen und etwa Handlungsempfehlungen für das Verhalten im Netz zu formulieren (z. B. Grimm/Schuster o. J.).

51.2 Geschichte und Institutionalisation

Fragen rund um die Ethik der digitalen Technologien haben deren Entwicklung von Beginn an begleitet und gehen somit zurück bis in die 1940er und 1950er Jahre. Damals nahm die Forschung zu Informationstechnologien und Künstlicher Intelligenz ihren Anfang. Schon Joseph Weizenbaum, der 1966 einen der ersten Chatbots programmierte, staunte über den Effekt der recht simpel gestrickten Maschine auf Menschen, die mit dem Bot kommunizierten, und legte eine ausführliche Kritik der Verführungskräfte der digitalen Technologien vor (Weizenbaum 1977). Inzwischen ist unstrittig, dass der Einsatz der datenbasierten Technologien einer gesetzlichen Regelung, aber auch eigener ethischer Reflexion bedarf. Das äußert sich auf politischer Ebene etwa in der Einrichtung der Enquete-Kommission „Künstliche Intelligenz“ durch den Deutschen Bundestag und der Datenethikkommission der Bundesregierung 2018, verschiedene Gremien auf der Ebene der Bundesländer und die High Level Expert Group on AI der Europäischen Kommission. Darüber hinaus befassen sich zahlreiche Nichtregierungsorganisationen, Berufsverbände, Unternehmen und Zusammenschlüsse von Wissenschaftlern mit der Frage, wie diese Technologie reguliert werden kann und muss, um sicherzustellen, dass sie zum Wohl

der Gesellschaft eingesetzt wird. Ethische Fragen finden zudem immer häufiger Eingang in die Ausbildung von Informatikern, an immer mehr Universitäten entstehen eigene Institute oder Lehrstühle für Digitale Ethik, immer mehr Firmen und Berufsverbände entwickeln eigene Ethikrichtlinien, für die Entwicklung von automatisierten Entscheidungssystemen, ihre Transparenz und Kontrollierbarkeit, und machen auf Mögliche Einseitigkeiten, („biases“) der Systeme aufmerksam.

Die politische Regulierung der Digitalisierung erfordert ebenso wie die ethische Reflexion zunächst ein mit der technologischen Entwicklung schritthaltenes technisches Verständnis. Schon deswegen handelt es sich bei der Digitalen Ethik um ein interdisziplinäres Unterfangen, bei dem außer Philosophen auch Juristen und Ingenieure, Psychologen und insbesondere natürlich Informatiker gefragt sind. Da die Auswirkungen der digitalen Technologien in vielen Bereichen noch gar nicht genau genug bekannt sind, besteht ein Teil der Arbeit an Instituten für Digitale Ethik in empirischen Analysen, etwa über die Auswirkungen der Handynutzung auf das Selbstbild. Hinzu kommen bisweilen Anleihen aus dem Bereich der Experimentellen Philosophie, etwa wenn erforscht werden soll, welche Entscheidungen Menschen in welchen Situationen für angemessen halten, um daraus eine Grundlage zur Programmierung algorithmischer Entscheidungssysteme zu gewinnen.

Weiterhin überwinden die digitalen Technologien geografische, politische und teilweise auch sprachliche und kulturelle Grenzen, was regionale und nationale Regulierungsbemühungen erschwert, Pluralität zur Grundbedingung jeder digitalen Ethik macht und die Verabsolutierung einzelner kultureller Traditionen verbietet. Schließlich verbinden sich mit den digitalen Technologien zugleich große Hoffnungen und große Ängste: Die Hoffnung auf eine egalitäre, demokratische Weltgesellschaft auf der einen Seite und die Sorgen um die Vertiefung der Kluft zwischen Arm und Reich, die Ausbeutung der Daten für kommerzielle Zwecke und ihr Missbrauch für Manipulation und Überwachung auf der anderen.

51.3 Zentrale Themen

Die Digitale Ethik umfasst ganz unterschiedliche Themenfelder. Den „zentralen Konflikt moderner Informations- und Wissensgesellschaften“ sieht Kuhlen in den antagonistischen Konzepten von Forum und Markt: „Wissen und Information können so umfassend und freizügig wie nie zuvor in der Geschichte der Menschheit allen bereitgestellt werden – faktisch ist jedoch der Zugriff auf Wissen und Information nie so kompliziert und begrenzt gewesen wie heute in der fortschreitenden Kommerzialisierung von Wissen und Information“ (Kuhlen 2004a, 34). Zu den am häufigsten behandelten Themen zählen derzeit:

Neue Werte für eine neue Gesellschaft: Viele der Probleme, die im Kontext der Digitalisierung diskutiert werden, wurden von dieser nicht hervorgerufen, aber verstärkt. So ermöglicht das Sammeln und Auswerten von immer mehr Daten die immer weitergehende Durchdringung und Optimierung ökonomischer und sozialer Prozesse. Zudem neigt die Digitalwirtschaft zur Bildung von Monopolen: Wer bereits große Mengen an Daten besitzt, kann seine Dienste zielgerichteter anbieten und auf diese Weise noch mehr Daten generieren. Zudem machen die Datenspuren, die wir alle in den digitalen Medien ziehen, uns mehr oder weniger durchsichtig, kontrollierbar und manipulierbar. Die zentrale Frage ist nun, wie die Vorzüge der digitalen Technologie genutzt werden können, ohne die Entwicklung in Richtung auf einen Überwachungsstaat oder einen Monopolkapitalismus zu befördern. Muss die Gesellschaft ihre grundlegenden Werte neu formulieren? Benötigt sie neue Werte? Menschenwürde, Freiheit, Autonomie und Verantwortung, aber auch die Frage nach dem guten Leben sind im Kontext der Digitalen Ethik hoch aktuell. Bisweilen ist von der Notwendigkeit einer neuen Aufklärung oder eines neuen Gesellschaftsvertrags die Rede.

Datenschutz und der Schutz der Privatsphäre: Je mehr Daten, desto besser: das ist das Credo der Datenwirtschaft. Speicherplatz ist billig, also wird erst einmal gesammelt, was zu

bekommen ist, auch wenn noch nicht absehbar ist, wozu diese Daten einmal gebraucht werden könnten. Bei rechtmäßig gesammelten Daten stellt sich hier die Frage der Datensicherheit: Werden sie so gespeichert und verarbeitet, dass sie nicht in falsche Hände geraten? Mindestens ebenso dringend ist die Frage nach dem Schutz der Privatsphäre. Das Sammeln von Daten über Personen und der Handel mit möglichst detaillierten Profilen ist längst zu einem riesigen Markt und einem verbreiteten Geschäftsmodell geworden. Dabei geht es vor allem um die nutzerspezifische Adressierung von Werbung.

Sorge bereitet hier vor allem die Konzentration und Vernetzung ganz unterschiedlicher Daten in den Händen großer Suchmaschinenbetreiber, Onlinehändler und App-Betreiber. Hinzu kommen Daten der immer zahlreicher werdenden Überwachungskameras. War im analogen Zeitalter das Durchsuchen großer Datenbestände schon durch den Zeitaufwand beschränkt, ist heute das Erinnern und Verknüpfen leichter und billiger als das Löschen und Vergessen. Dies eröffnet Konzernen, aber auch staatlichen Stellen unabsehbare Kontroll- und Manipulationsmöglichkeiten. Während wenige argumentieren, das Konzept der Privatsphäre sei nicht mehr zeitgemäß (Heller 2011), versuchen die meisten in diesem Bereich Engagierten, technische und juristische Lösungen zu finden, um Datenschutz und Privatsphäre unter den Bedingungen der Digitalisierung zu gewährleisten. Diese Bemühungen kollidieren nicht nur mit den Bestrebungen der großen Internetkonzerne, immer mehr Daten über ihre Nutzer zu erfassen, sondern auch mit den Interessen etwa der biologischen, medizinischen oder soziologischen Forschung, durch die Analyse großer Datenmengen neue Erkenntnisse zu gewinnen. Modelle wie etwa die Datenspende oder der Datentreuhänder werden derzeit diskutiert, um den Interessen der Forschung und dem Datenschutz und der Datensouveränität der Menschen zugleich Rechnung zu tragen. Welche Beschränkungen der Informationssammlung und -speicherung erforderlich sind, um eine freiheitliche Gesellschaft aufrechtzuerhalten, ist Gegenstand der Informationsökologie (Mayer-Schönberger 2010).

Diskriminierung durch Algorithmen: Algorithmische Entscheidungssysteme auf der Basis von Verfahren des maschinellen Lernens (s. Kap. 118) spiegeln die Struktur der Daten, mit denen sie trainiert wurden. Diese enthalten oft Einseitigkeiten, wodurch die Algorithmen Strukturen entwickeln können, die Personen oder Personengruppen benachteiligen. Zudem ist schwer nachzuvollziehen, wie diese Systeme zu ihren Ergebnissen kommen. Was bei eher technischen Fragen ein Sicherheitsrisiko darstellen kann, ist bei Systemen, die Entscheidungen fällen, von denen Menschen betroffen sind, meist nicht akzeptabel.

Jugendschutz: Ein Thema des Jugendschutzes ist der technisch nur schwer einzuschränkende Zugang zu jugendgefährdenden Inhalten. Ein anderes Thema sind die Nebenwirkungen von übertriebenem Computerspielen wie Sucht, Realitätsverlust, Vereinsamung, geringes Selbstwertgefühl durch ständiges Online-Vergleichen, Verzerrung der Wirklichkeitswahrnehmung und die Einschränkung der Fähigkeit, mit Menschen zurechtzukommen. Hierher gehört auch die Gefahr, dass Kinder und Jugendliche durch ihr spezifisches Kommunikationsverhalten private Informationen einem unbeschränkten Kreis von Personen preisgeben, ohne absehen zu können, wie ihnen das zum Nachteil gereichen könnte (Hausmanninger 2003).

Neue Straftatbestände: Bestimmte Straftatbestände werden durch die neuen Informations- und Kommunikationstechnologien erst ermöglicht, wie etwa der Betrug mit Passwörtern und der Diebstahl von persönlichen Profilen und Identitäten. Andere werden durch diese Technologien erleichtert oder in einem zuvor unbekanntem Ausmaß möglich, wie das Verabreden von Straftaten oder die Verbreitung von Kinderpornografie. Mit dem Internet sind auch Phänomene wie das Cyber-Stalking und das Cyber-Mobbing (Tavani/Grodzinsky 2004) und die digitale Hassrede (hate speech) entstanden.

Mit zunehmender Digitalisierung der Infrastruktur sind auch Manipulationen von und Angriffe auf Infrastruktureinrichtungen, aber auch private Firmen und öffentliche Verwaltungen zu einem zentralen Thema geworden. Eine eigene

Behörde, das Bundesamt für Sicherheit in der Informationstechnik (BSI), befasst sich seit 1991 mit der Abwehr solcher Angriffe und hat heute über 1500 Mitarbeiter.

Wichtiger wird auch das Verbreiten illegal beschaffter geheimer Daten, wie etwa Wikileaks es mit aufklärerischem Anspruch praktiziert.

Manipulationen, Fakes und Filterblasen: Falschnachrichten (*fake news*), gefälschte Bilder oder Filme (*deep fakes*) sind in vielen sozialen Medien zu wichtigen Themen geworden. Immer wieder wird diskutiert, inwieweit diese Techniken etwa verwendet werden oder wurden, um Wahlen zu beeinflussen. Diskutiert wird auch, inwieweit die bloße Sorge oder der Verdacht, solche Techniken könnten eingesetzt werden, schon ausreicht, um Diskurse zu verändern und Vertrauen zu untergraben.

Hinzu kommt die Sorge, die Personalisierung von Nachrichten und Suchanfragen im Internet könnten dazu führen, dass Menschen vor allem Nachrichten angezeigt bekommen, die ihre bestehende Meinung bestätigen und sich so in „Filterblasen“ einschließen, die ihnen ein verzerrtes Bild der Welt vermitteln und die dazu beitragen, dass die Gesellschaft immer weiter in Teilgruppen zerfällt, die nicht mehr miteinander kommunizieren (Pariser 2012).

Die unüberschaubare Vielfalt von Informationen, die die digitalen Medien bereithalten, bietet Chancen und Risiken zugleich. Sie macht Wissen allgemein zugänglich, das zuvor bestimmten Berufsgruppen vorbehalten und, wenn überhaupt, nur unter großen Mühen zu bekommen war. Es ermöglicht den weltweiten Erfahrungsaustausch mit anderen Menschen. Daher war die Entstehung des Internets mit großen Hoffnungen für die Demokratisierung von Wissen und Informationen einher. ‚E-Democracy‘ steht für neue digitale Möglichkeiten demokratischer Teilhabe und Organisation.

Allerdings ist das Internet nicht zu dem herrschaftsfreien Raum geworden, von dem seine frühen Protagonisten träumten, sondern zu einem Feld, auf dem einige wenige große Konzerne um die Möglichkeiten konkurrieren, immer mehr Daten zu sammeln, um Werbung

gezielter schalten und Angebote besser personalisieren zu können.

Hier stellt sich immer dringender die Frage, ob der Staat verpflichtet ist, eine unabhängige digitale Infrastruktur für seine Bürger aufzubauen, damit sie an der politischen Willensbildung teilhaben können, und die nach einer Pflicht zum Schutz von nicht-kommerzialisierten Räumen und sprachlicher und kultureller Vielfalt im Netz.

Zensur: In engem Zusammenhang mit der Frage nach der geeigneten Bekämpfung von digital verbreiteten Falschnachrichten und Hassrede steht die Debatte um Zensur im Internet. Welche Filtermaßnahmen, Speicherungen von Verbindungsdaten, Seitensperrungen oder Überwachungsverfahren sind angemessen und wer soll sie durchführen? Dürfen Entscheidungen über zu sperrende Inhalte an private Firmen delegiert werden, dürfen sie von Maschinen getroffen werden? Welchen Einfluss üben zudem Suchmaschinen und Ratingverfahren auf die Zugänglichkeit von Informationen aus, wer beeinflusst bzw. bezahlt sie? Eine Herausforderung ist dabei die Balance zwischen dem Eindämmen unerwünschter oder krimineller Inhalte und der Meinungsfreiheit, eine andere die Einhaltung der unterschiedlichen nationalen Regelungen.

Haftung- und Zurechenbarkeit: Haftungs- und Zurechenbarkeitsfragen sind im digitalen Umfeld häufig schwer zu klären, da eingestellte Informationen oft keiner konkreten Person zugeordnet werden können. Doch ohne individuelle Zurechenbarkeit fehlt der Strafverfolgung, aber auch der moralischen Reflexion von Handlungen ihre Basis (Kuhlen 2004a). Je autonomer intelligente Systeme entscheiden dürfen, desto stärker rückt die Zurechenbarkeit und damit auch die Frage nach der Schuld in den Hintergrund. An ihre Stelle treten Konzepte wie die der elektronischen Person, analog zu der Rechtfigur juristischen Person. Der Grundgedanke: Ein solches (teil-)autonomes System soll nur mit einer ausreichend ausgestatteten Versicherung in den Verkehr gebracht werden dürfen, so dass eine Person, der ein Schaden entsteht, immerhin diesen ersetzt bekommt, auch wenn niemand

persönlich für das Geschehen haftbar gemacht werden kann (Hilgendorf 2015).

Geistiges Eigentum und Copyright: Eines der wichtigsten Themen in der Debatte um die Gestaltung der digitalen Medienwelt ist der Umgang mit geistigem Eigentum und Copyright. Ist alles Wissen Besitz der Menschheit und muss deshalb für alle frei zugänglich sein, oder ist es gerechtfertigt, den Zugang zu Informationen zu beschränken und im Internet wie in klassischen Printmedien zu verkaufen? Diese Frage beschäftigt die mit der Regulierung des Internet befassten Gremien auf nationaler wie internationaler Ebene und ist mit massiven wirtschaftlichen Interessen verbunden.

Zugang zur digitalen Welt: Da der ungehinderte Zugang zu Informationen in einer Wissensgesellschaft eine zentrale Rolle spielt, ist der gleichberechtigte Zugang zum Internet eine wichtige Ressource für die Teilhabe am gesellschaftlichen Leben und für Chancen auf dem Arbeitsmarkt. Doch diese Zugangsgerechtigkeit ist weder national, innerhalb der Industriestaaten, gegeben, noch international in der Beziehung zu den zu Schwellen- und Entwicklungsländern. Dies wird als digitale Spaltung oder digitale Kluft (*digital divide, digital gap*) bezeichnet (Scheule et al. 2004). Dabei geht es um den Zugang zur nötigen technischen Ausstattung, aber auch um die Ausbildung, die es Menschen erst ermöglicht, effizient und kritisch mit den angebotenen Informationsmengen umzugehen. So nutzen Statistiken zufolge in Europa und Nordamerika fast 90 % der Bevölkerung das Internet, in Afrika hingegen nur 40 %, wobei Afrika und der Mittlere Osten die höchsten Zuwachsraten aufweisen.

Digitale Medien zu nutzen ist allerdings nicht mit Digitalkompetenz gleichzusetzen. Nur 20 % der Bevölkerung der Bundesrepublik gab in Umfragen an, sich für die Hintergründe und Trends der digitalen Technologie zu interessieren (D21-Digital-Index).

Individualisierung und Überforderung: Die Möglichkeiten, die die Informations- und Kommunikationstechnologien bieten, stellen immer höhere Anforderungen an die Fähigkeiten der Nutzer, auszuwählen, zu bewerten und das

Leben angesichts der angebotenen Vielfalt auf befriedigende Weise zu organisieren. Die ständige Verfügbarkeit der allerneuesten Informationen (*information overload*; vgl. Levy 2008) führt zu einer scheinbaren Entwertung von Erlerntem, von Alltags- und Lebenserfahrungen (Bergsdorf 2002). Dabei gerät zum einen leicht in Vergessenheit, dass die Fähigkeit, wichtige und gute Informationen auszuwählen, gerade von einer guten Ausbildung und dem dazu gehörenden Wissen abhängt (Informationskompetenz, *information literacy*). Da aber längst nicht alle Menschen eine solche Ausbildung erhalten, vertieft dieser Aspekt die digitale Spaltung. Zum anderen muss kritisch gefragt werden, ob die neuen Wahlmöglichkeiten vom Individuum in einer sinnvollen Weise genutzt werden können. Charles Ess sieht die Gefahr, dass die allzu leicht verfügbaren Informationsmengen die Menschen nicht zu individuelleren und kritischeren, sondern zu gleichgültigeren Bürgern machen. Am Ende, so befürchtet er, könnten digitale Kommunikations- und Informationstechnologien die Demokratie ruinieren, statt sie zu stärken, indem sie die Fähigkeit zu kritischem Denken untergraben (Ess 2010).

Hinzu kommt der Drang zur Optimierung des eigenen Lebens, befördert durch Apps, die das Vermessen des eigenen Lebens, sportlicher Leistungen ebenso wie des Ess- und Schlafverhaltens oder medizinischer Daten ermöglichen und nahelegen. Auch die ständige Bewertung von Leistungen und des Auftritts in sozialen Medien kann Stress erhöhen und zur Überforderung des Individuums beitragen.

Weitere Themen: Zu den Themen der digitalen Ethik gehören auch die Mensch-Maschine-Interaktion und die Frage, in welchen Bereichen (etwa in der Pflege) welche Systeme eingesetzt werden sollten oder nicht eingesetzt werden dürfen; Fragen nach den Auswirkungen der Digitalisierung auf dem Arbeitsmarkt und das große Gebiet der autonomen Waffensysteme.

Vom Anspruch her ist die junge Disziplin Digitale Ethik eine Bereichsethik, aber eine solche, die für einen immer wichtiger werdenden Bereich des öffentlichen wie privaten Lebens zentrale ethische Frage zu beantworten versucht:

Wie wollen wir leben? Welche Welt wollen wir unseren Kindern hinterlassen? (Kuhlen 2004b). Auch angesichts der in vielen Hinsichten neuen Situation, wie sie die Digitalisierung mit sich bringt, erfüllt die Ethik hier ihre traditionelle Rolle der Reflexion und fragt nach den Möglichkeiten von Verantwortung Moral und Freiheit.

Literatur

- Bergsdorf, Wolfgang: Ethik in der Informationsgesellschaft. Paderborn 2002.
- Capurro, Rafael: „Digitale Ethik“. In: <http://www.capurro.de/DigitaleEthik.html> (10.4.2020).
- D21-Digital-Index 2016: Jährliches Lagebild zur Digitalen Gesellschaft. In: <https://initiatedv21.de/app/uploads/2017/01/studie-d21-digital-index-2016.pdf> (10.4.2020).
- Ess, Charles: „Brave New Worlds? The Once and Future Information Ethics“. In *International Journal of Information Ethics* 12. Jg., 3 (2010), 36–44.
- Frohmann, Bernd: „Cyberethik. Bodies oder Bytes?“ In: Thomas Hausmanninger, Rafael Capurro (Hg.): *Netzethik. Grundlegungsfragen der Internetethik*. München 2002, 49–60.
- Greis, Andreas: „Strukturanalyse als Weg zu einer Internetethik.“ In: Thomas Hausmanninger/Rafael Capurro (Hg.): *Netzethik. Grundlegungsfragen der Internetethik*. München 2002, 123–140.
- Grimm, Petra/Keber, Tobias/Zöllner, Oliver: *Digitale Ethik. Leben in vernetzten Welten*. Reclam 2019.
- Grimm, Petra/Schuster, Wolfgang (o.J.) 10 Gebote der Digitalen Ethik. In: https://www.hdm-stuttgart.de/digitale-ethik/lehre/10_gebote (21.3.2022).
- Grimm, Petra/Hammwöhner, Rainer/Wolff, Christian: „Gesellschaftliche und interdisziplinäre Aspekte der Informatik.“ In: Michael Henninger/Heinz Mandl (Hg.): *Handbuch Medien- und Bildungsmanagement*. Weinheim 2009, 272–287.
- Hausmanninger, Thomas (Hg.): *Handeln im Netz. Bereichsethiken und Jugendschutz im Internet*. München 2003.
- Heller, Christian: *Post-Privacy. Prima leben ohne Privatsphäre*. München 2011.
- Hilgendorf, Eric: Recht und autonome Maschinen – ein Problemaufriss. In: Eric Hilgendorf/Sven Hötitzsch (Hg.): „Das Recht vor den Herausforderungen der modernen Technik.“ In: *Robotik und Recht*. Bd. 4. Baden-Baden 2015, 11–40.
- Hilgendorf, Eric/Capurro, Rafael (Hg.): *Netzethik. Grundlegungsfragen der Internetethik*. München 2002.
- Himanen, Pekka: *Die Hacker-Ethik und der Geist des Informationszeitalters*. München 2001.
- Hustedt, Carla: Algorithmen fürs Gemeinwohl: 10 Erkenntnisse aus 2 Jahren intersektoraler Arbeit. Bertelsmannstiftung 2019. In: <https://www.bertelsmann-stiftung.de/unsere-projekte/ethik-der-algorithmen/projektnachrichten/algorithmen-fuers-gemeinwohl-10-erkenntnisse-aus-2-jahren-intersektoraler-arbeit/> (10.4.2020)
- Kolb, Anton/Esterbauer, Reinhold/Rückenbauer, Hans Walter (Hg.): *Cyberethik. Verantwortung in der digital vernetzten Welt*. Stuttgart 1998.
- Kuhlen, Rainer: *Informationsethik. Umgang mit Wissen und Informationen in elektronischen Räumen*. Konstanz 2004a.
- Kuhlen, Rainer: „Informationsethik.“ In: Rainer Kuhlen/Thomas Seeger/Dietmar Strauch (Hg.): *Grundlagen der praktischen Information und Dokumentation*. München 2004b, 61–71.
- Levy, David: „Informational Overload.“ In: Kenneth Einar Himma/Herman T. Tavani (Hg.): *The Handbook of Information and Computer Ethics*. New Jersey 2008, 497–515.
- Mayer-Schönberger, Viktor: *Delete. Die Tugend des Vergessens in digitalen Zeiten*. Berlin 2010.
- Pariser, Eli: *The Filter Bubble. What the Internet is Hiding from You*. Penguin 2012.
- Scheule, Rupert M./Capurro, Rafael/Hausmanninger, Thomas (Hg.): *Vernetzt gespalten. Der Digital Divide in ethischer Perspektive*. München 2004.
- Spiekermann, Sarah: *Digitale Ethik. Ein Wertesystem für das 21. Jahrhundert*. München 2019.
- Tavani, Herman T./Grodzinsky, Frances S.: „Ethical reflections on Cyberstalking“. In: Richard A. Spinello/Herman T. Tavani (Hg.): *Readings in CyberEthics*. London 2004, 561–570.
- Weber, Karsten: „Informationelle Gerechtigkeit. Herausforderungen des Internets und Antworten einer neuen Informationsethik.“ In: Helmut F. Spinner/Michael Nagenborg/Karsten Weber: *Bausteine zu einer Informationsethik*. Berlin 2001, 129–194.
- Weber, Karsten: „Grundlagen der Informationsethik. Politische Philosophie als Ausgangspunkt informationsethischer Reflexion.“ In: Thomas Hausmanninger/Rafael Capurro (Hg.): *Netzethik. Grundlegungsfragen der Internetethik*. München 2002, 141–156.
- Weizenbaum, Joseph: *Die Macht der Computer und die Ohnmacht der Vernunft*. Frankfurt a.M. 1977 (engl. 1976).
- www.internetworldstats.com.