Einsatz jeweils an Hand der aus unserer Verfassungsordnung abzuleitenden *Prinzipien eines rechtsstaatlichen Strafverfahrens* zu überprüfen, wozu der Schutz der Menschenwürde und die Garantie der informationellen Selbstbestimmung ebenso gehören wie die Unschuldsvermutung, das Recht, sich nicht selbst belasten zu müssen, und die Garantie eines fairen Verfahrens. Werden diese übergreifenden Prinzipien nicht beachtet, so erodiert das Vertrauen der Bevölkerung in die Objektivität und Grundrechtsorientierung unserer Strafverfolgung. Zweifel hieran würden für die Effektivität der Strafverfolgung einen größeren Schaden verursachen als der Einsatz neuer technischer Ermittlungsmöglichkeiten.

1 *z.B. Rath, taz 18.01.2005.*
2 *Kieler Nachrichten 15.01.2004, 7, „Buß will Verbrecher im Labor überführen".*
3 *z.B. Bund Deutscher Kriminalbeamter (BDK) LV Schleswig-Holst. Presseerklärung v. 09.01.2004*
4 *DatenschutzNachrichten (DANA) 1/2003, 32.*
5 so Wagner, Zeitschrift für Rechtspolitik 2004, 14.
6 *Der Spiegel 45/2002, 303; DANA 4/2000, 32.*
7 *z.B. Diabetes-Risiko, DANA 3/2001, 26 f.*
8 *DANA 2/202, 37.*
9 *Der Spiegel 45/2002, 204; DANA 4/2002, 31.*
10 *BVerfG NJW 2001, 880; BVerfG NJW 2001, 2321.*
11 *Koydl Süddeutsche Zeitung vom 12.11.2003, 11.*
12 *dpa-Meldung 06.02.2004.*
13 *DANA 1/2003, 32.*
14 *zu Frankreich DANA 1/2003, 32 f.; Großbritannien DANA 4/2000, 32, DANA 1/2000, 24, DANA 1/1999, 30 f.; Österreich DANA 1/2000, 24; Schweiz DANA 2/1999, 38; USA, DANA 1/1999, 32 f.*
15 *DANA 1/2001, 29.*
16 *so eine BKA-Studie von Ende 2002, zit. nach DANA 1/2003, 32.*
17 *BVerfG NJW 2001, 881 f.; BVerfG NJW 2001, 882 f.; BVerfG NJW 2001, 2321; zur Dokumentationspflicht 25. Tätigkeitsbericht (TB) 2003 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD SH), Kap. 4.2.2.*
18 *Nowak www.telepolis.de 13.02.2004.*
19 *anders die Justizminister Weiß, Bayern, und Wagner, Hessen, Der Spiegel 27/2003, 22, DANA 3/2003, 16.*
20 *BVerfG NJW 1969, 1707; dazu ausführlich Weichert Recht der Datenverarbeitung 2002, 170 ff.*
21 *Schild, DANA 3/2003, 5 ff.*
22 *DANA 2/2002, 36.*
23 *Statewatch vol 13 no 1 january-february 2003, 2; DANA 2/2003, 27.*
24 *so z.B. im ersten bei 1.300 Frauen durchgeführten Gentest in Bayern 2003, DANA 2/2002, 36; Der Spiegel 12/2003, 52; LG Regensburg DANA 2/2003, 37.*
25 *BVerfG NStZ 1996, 345.*
26 *so z.B. ein Verfahren in Sachsen, DANA 4/2002, 30; bei einem Massentest in Niedersachsen an 18.000 Männern war die Tätersuche erfolgreich, DANA 4/1998, 2; dazu kritisch Dronsch/Sokol, DANA 1/1999, 28; Deutsche Vereinigung für Datenschutz (DVD), DANA 2/1998, 27.*
27 *Satzger JZ 2001, 639 ff.*
28 *DANA 2/2002, 30; 25. TB 2003 ULD SH, Kap. 4.2.3.*
29 *23. TB 2001 ULD SH, Kap. 4.3.2*
30 *siehe die Diskussion über das „Prügel-Gen" von Prinz Ernst August, DANA 2/2000, 16 f.*
31 *DANA 4/2001, 29.*
32 *DANA 2/2003, 28.*

Eva Hornecker und Peter Bittner

Jenseits von Whistleblowing

In der Diskussion um ethische Fragen der Informatik fällt, wenn es um die Berufspraxis geht, häufig der Begriff des „Whistleblowing". Damit werden Situationen bezeichnet, in denen Angestellte die Öffentlichkeit vor Risiken warnen, die ihre Arbeitgeber verursachen. Um Studierende für ihre berufliche Verantwortung zu sensibilisieren, werden solche Fallbeispiele gerne in der Lehre diskutiert und in Lehrbücher zu Computer-Ethics einbezogen. Wir halten diese Fokussierung auf das Whistleblowing für falsch und sogar für kontraproduktiv und werden dies im folgenden Essay begründen. Notwendig erscheint uns ein anderer Ansatz, der die Alltagspraxis ernst nimmt und sich für die Grauzonen der Ethik und die scheinbar unwichtigen, kleinen, alltäglichen Entscheidungen interessiert.

Whistleblowing entspricht dem Signal einer Pfeife (whistle), die vor einer drohenden Gefahr warnt oder eine Tätigkeit abrupt stoppt (Schiedsrichterpfiff, Warnpfiff der Polizei zur Alarmierung derr Öffentlichkeit und Herbeirufen anderer Polizisten). Ist einem Arbeitnehmer eine Gefährdung der Öffentlichkeit durch das Verhalten oder die Fahrlässigkeit seines Arbeitgebers bekannt, sollte er die Öffentlichkeit vor diesem Risiko warnen können.[1] Damit verletzt er oder sie jedoch zugleich arbeitsvertraglich festgelegte Loyalitäts- Treue- und Verschwiegenheitspflichten. Daher sieht das amerikanische Recht das Konstrukt des *Whistleblowing* vor, welches den Arbeitnehmer (zumindest prinzipiell) vor der Kündigung schützt. Faktisch ist die Lage komplizierter, denn meist muss der Arbeitnehmer nachweisen, dass die Kündigung eine Vergeltungsmaßnahme ist (Hersh 2002).

Das deutsche Recht sieht so etwas nicht vor, obgleich die Gerichte häufig ihren Ermessensspielraum zu Gunsten des Arbeitnehmers nutzen (Däubler 2000).

Zu einem Trendbegriff (Müller 2004) wird Whistleblowing unter anderem deswegen, weil ein neues US-Gesetz[2] börsennotierte Aktienunternehmen zwingt, kritische Mitarbeiter besser zu schützen. Betroffen sind auch deutsche Unternehmen, sofern sie an US-Börsen notiert sind. Dies wird auf längere Sicht Druck auf die deutsche Rechtssprechung ausüben. Besagtes Gesetz betrifft allerdings nur den Schutz von Angestellten, die Verstöße gegen Bilanzvorschriften offenlegen (falsche Darstellungen in der Finanzberichtsdarstellung des Konzerns).

Geht es um die gesellschaftliche Verantwortung von Informatikern oder Ingenieuren, fällt der Begriff des Whistleblowings häufig. Auch in der Lehre werden gerne Fälle des Whistleblowing diskutiert, um Studierende für ihre spätere berufliche Verantwortung zu sensibilisieren. Unseres Erachtens greift dies jedoch zu kurz und verstellt den Blick auf wichtige ethische Aspekte der Berufspraxis. Plakativ verkürzt: Im Falle von Whistleblowing ist das Kind bereits in den Brunnen gefallen. Ist es klug, sich hauptsächlich mit derartigen Krisenfällen zu beschäftigen – zumal es sich bei diesen Fällen nur um die Spitze eines Eisberges handelt?

Wir glauben, dass es viel produktiver ist, eine mikroethische Sicht einzunehmen und ein Bewusstsein für Arbeitskulturen, Denk- und Handlungsmuster der Informatik zu kultivieren. Dies bedeutet, dass auch die Forschung zu *Computer Ethics* ihren Blick stärker auf die Alltagspraxis der Informatik und die täglichen, kleinen, konkreten Designentscheidungen richten sollte (vgl. Kling 1996, Hanseth und Monteiro 1994), anstatt sich vorrangig mit Spezialthemen wie Privacy, Hacken und Software-Piraterie zu befassen.

Lynch und Kline (2000) haben für das Ingenieurswesen analysiert, wie Arbeitskulturen und scheinbare Routineentscheidungen langfristig zu ungewollten negativen Ergebnissen führen können, ohne dass Verantwortliche festgemacht werden können. Sich wiederholende, für sich gesehen scheinbar rationale Handlungen legen einen Verlauf fest, von dem abzuweichen später schwer fällt. Denn im Laufe der Zeit ist eine bestimmte Denk- und Arbeitskultur entstanden, die das *Normale* bestimmt. Wer immer billige Ersatzteile kauft, hat irgendwann nur noch Billigware, wer immer wieder Risiken in Kauf nimmt, wird irgendwann unvorsichtig und verliert das Augenmaß … Moralische Dilemmata haben eine lange Inkubationszeit, sie werden *ausgebrütet*. Sie rechtzeitig zu erkennen, verlangt ethisches Urteilsvermögen; auf sie zu reagieren verlangt Improvisationsvermögen, Feingefühl und soziale Kreativität.

Arbeitnehmer sind in Arbeitskulturen eingebunden, die den *normalen* Handlungsraum bestimmen. Zugleich stellen sie diese Arbeitskulturen aktiv (wieder) her. Darin besteht immer auch die Möglichkeit der Veränderung. Notwendige Fähigkeiten – und damit sinnvolle Ziele für Ethik in der Lehre – sind daher das Erkennen impliziter Annahmen und alltäglicher ethischer Fragen in schlecht strukturierten Problemfeldern sowie die kreative Lösungsfindung. Es geht um präventive Ethik anstelle einer Krisenethik (vgl. Lynch und Kline 2000).

Eva Hornecker, Visiting Research Fellow an der University of Sussex

Peter Bittner, Humboldt Universität zu Berlin, Institut für Informatik

Risiken der Fokussierung auf Whistle Blowings und *große* ethische Fragen

Lynch und Kline (2000) warnen sogar davor, Fälle des Whistleblowing in der Lehre zu diskutieren. Studierenden solche *Alles-oder-Nichts*-Fälle vorzulegen, vermittle ihnen das Gefühl, dass es bei Ethik immer nur um einen "Trade-off between sacrificial heroism and amoral self-interest" gehe. Die Beschreibung dieser Fälle verschweige meist die lange Vorgeschichte und mache damit eine Diskussion über die Möglichkeit anderer Handlungspfade unmöglich.

Die Wahrscheinlichkeit, in der eigenen Berufspraxis in eine solche Lage zu geraten, in der tatsächlich eine Gefährdung der Öffentlichkeit (von Leib, Leben, Gesundheit) oder ein massiver Gesetzesbruch besteht, ist (hoffentlich) eher gering. Betrachtet man Versuche von Fachgesellschaften, zu definieren, wann die Handlung des Whistleblowing als gerechtfertigt gelten kann (z.B. die British Computer Society: *http://www.bcs.org/BCS/Groups/ExpertPanels/Ethics/whistle.htm*), so sind die Ansprüche an den Handelnden sehr hoch. Viele Aspekte lassen sich nicht objektiv überprüfen.

Dennoch finden sich Berufspraktiker immer wieder in Situationen, die ihnen *Bauchschmerzen* bereiten, in denen sie entgegen ihren Überzeugungen handeln müssen oder Bedenken haben (siehe auch Kling 1996). Diese Bedenken können beispielsweise die Usability oder Stabilität eines Produkts betreffen, das termingerecht fertiggestellt werden muss, damit das Projekt rentabel bleibt. Arbeitnehmer finden sich in massiven Interessenkonflikten wieder und sollen dabei zuvorderst die Interessen ihres Arbeitgebers vertreten. So berichtet in der Umfrage von Hornecker und Bittner (2000) ein im Bereich Outsourcing angestellter IT-Berater, dass er auch solchen Kunden das Outsourcing nahe legen muss, denen er ehrlicherweise davon abraten sollte.

Verlangt man verantwortungsvolles Verhalten von IT-Berufspraktikern, so muss man auch die Frage nach der Verhältnismäßigkeit der Konsequenzen stellen. Werden beim Entwurf eines Informatik-Systems beispielsweise datenschutzrechtliche Bestimmungen missachtet, ohne dass dies im praktischen Systemeinsatz ausgenutzt wird, so ist dies ein Gesetzesverstoß, der noch keine *akute Gefährdung* darstellt. Der Arbeitnehmer sollte

seine Vorgesetzten auf diesen Verstoß hinweisen. Kann man von ihm weitere Schritte verlangen, den Kunden und potenziell vom System Betroffene zu informieren und damit das Vertrauensverhältnis zu gefährden sowie den eigenen Job aufs Spiel zu setzen?

Wer einmal aufgrund einer solchen Entscheidung gekündigt wurde und eventuell sogar gegen den Arbeitgeber prozessiert hat, wird es danach schwer haben, wieder eine Anstellung zu finden. Whistleblowing kann daher immer nur die letzte Konsequenz sein. Hersh (2002) kommt in ihrer Zusammenfassung verschiedener Studien denn auch zu dem Ergebnis, dass es vor allem durch undurchschaubare, indirekte und komplexe Kommunikationswege innerhalb eines Unternehmens, autoritäre Strukturen sowie die Unterdrückung von Zweifel oder Kritik als Charakteristika einer Organisation zu Whistleblowing kommt. Erschreckend ist auch, welche Konsequenzen diejenige Person erwarten. Hersh (2002) führt die Ergebnisse mehrer Umfragen und Studien zusammen. Laut einer Studie erfuhren von 87 US-amerikanischen Whistleblowern in staatlichen Organisationen und Privatindustrie alle bis auf eine Person offizielle Vergeltungsmaßnahmen sowie Schikanen durch Kollegen und Vorgesetze. Die Mehrheit verlor ihren Job, 17% das Haus, 8% mußten Bankrott anmelden, 15% wurden im Verlauf geschieden und 10% versuchten Selbstmord. In einer anderen Umfrage erfuhren 71% offizielle Vergeltungsmaßnahmen. Inoffizielle Vergeltung (91%) bestand aus der Ächtung am Arbeitsplatz, persönlichen Angriffen, verschärfter Kontrolle sowie Isolation und Ausgrenzung.

Hinzu kommt, dass Whistleblowing nicht besonders effektiv zu sein scheint. Die bisher veröffentlichten Studien geben allesamt, so Hersh (2002), keinen Beleg für die Erfolgsrate. Nur in wenigen Bereichen (die im öffentlichen und Medieninteresse standen) führte Whistleblowing zu politischen Veränderungen (AIDS-Diskriminierung, giftige Abfälle, Nuklearkraft). Hersh kommt darüber hinaus zu diesem Fazit: „Whistleblowing generally focuses on abuses within the system rather than challenging the nature of the system itself, which would require collective action (...). Whistleblowers challenge fraud, health and safety violations, but not the nature of their organisation's activities."

Der Einzelne steht zudem immer in einem Spannungsfeld der Verantwortung für verschiedene Bereiche. In unserer Umfrage (2000) verwiesen einige Berufspraktiker darauf, dass sie ihre Kollegen vor Mehrarbeit und eventuellem Jobverlust (z.B. im Fall einer für das Unternehmen bestandsgefährdenden Konventionalstrafe) schützen wollen, und dass im Ernstfall die Verantwortung für die eigene Familie schwerer wiege.

Redet man mit Berufspraktikern über ihre berufliche Verantwortung, so fällt auf, dass diese zunächst oft nicht bestimmen können, wo ihre Arbeit ethische Aspekte berührt, oder dass sie ihre Erlebnisse für unwesentlich und „zu klein" halten. Gerade Informatiker, die sich während ihres Studiums intensiv mit Fragen von Informatik und Gesellschaft befasst haben, wirken häufig desillusioniert und sehen wenig Handlungsspielraum – es könne nicht jeder „ein Weizenbaum" sein. Dies lässt uns vermuten, dass der Fokus der Diskussion in Wissenschaft und Lehre auf *große* ethische Probleme nicht zur Handlungsfähigkeit beiträgt und eher das Gegenteil eines überhöhten, nicht einlösbaren Anspruchs an sich selbst bewirkt. Eine weitere Folge ist offenbar, dass die alltäglichen kleinen Gewissenskonflikte als „vergleichsweise unwesentlich" bewertet werden und damit nicht zum Gegenstand ethischer Reflexion werden. Diese Geringschätzung der Alltagspraxis und des situierten moralischen Urteilens ist leider ein prinzipielles Problem der Ethik als akademischer Disziplin.

Der Blick auf die Alltagspraxis und die Arbeitskulturen

Sowohl Lynch und Kline (2000) als auch Forester (1999) raten dazu, die Alltagspraxis in der Lehre zu reflektieren. Gerade die Unordnung und Unklarheit von *echten* Geschichten aus der Praxis sei ihre Stärke. Es sind die Grauzonen der Alltagspraxis, in denen wir tagtäglich und nebenbei kleine ethische Entscheidungen treffen, welche letztlich bestimmen, was für Menschen wir sind, und wie wir miteinander leben, die bestimmen, wie unsere Fachdisziplin von ihren *Kunden* wahrgenommen wird. Anders als andere Disziplinen wie Medizin, Pädagogik, Mediation (ein hervorragendes Beispiel ist z.B. Forester 1999), übt sich die Informatik jedoch nicht in einer Reflexion ihrer Arbeitskultur und Verhaltensmuster. Sie versucht nicht, aus guten und schlechten Beispielen alltäglicher Praxis zu lernen. Die Forschung über die eigene Praxis wird nicht als ein wesentlicher Teil der Disziplin angesehen – im Gegenteil, sie wird ausgegrenzt und den Sozialwissenschaften überlassen.

Zu einer Reflexion der Arbeitskulturen der Informatik würde es beispielsweise gehören, die eigene Einstellung gegenüber Kunden und Endanwendern und den Umgang mit ihnen zu reflektieren. Das Bild des „*Users*" beeinflusst implizit die Entwurfsentscheidungen sowie das Verhalten von Entwicklern. Schlagworte wie der „Dümmste Anzunehmende User" werden gerne spaßhaft verwendet und in einer Arbeitsgruppe rasch zum gängigen Ausdruck. Die sich darin ausdrückende Geringschätzung des Endanwenders beeinflusst die allgemeine Einstellung gegenüber Anwendern – es wird leichter, sich über Beschwerden wegen schlechter Usability oder Systemabstürze und vermutete Programmfehler hinwegzusetzen. Eine solche Einstellung macht es unwahrscheinlich, dass man sich ernsthaft mit den Bedürfnissen der Endanwender auseinandersetzt oder diese gar bei der Produktentwicklung beteiligt. Zahlreiche andere Aspekte wären eine genauere Untersuchung wert und sollten auch in der Ausbildung von Studierenden bedacht werden. Es wäre beispielsweise wichtig, sich mit den sozialen und ethischen Aspekten der Anforderungsanalyse und frühen Phasen der Software-Entwicklung zu befassen, insbesondere da diese den Erfolg eines Projekts maßgeblich bestimmen.

Ein Teil der Reflexion informatischer Praxis, beziehungsweise der Vorbereitung auf die berufliche Verantwortung als IT-Praktiker, sollte zudem darin bestehen, die strukturellen Probleme gängiger Praxis in der IT-Industrie zu identifizieren, welche die Erkenntnis- wie Handlungsmöglichkeiten des Einzelnen einschränken (Bittner und Hornecker 2002). Für den Einzelnen ist dies wichtig, um (insbesondere als Berufsanfänger) die eigenen Handlungsmöglichkeiten besser beurteilen zu können und angemessen zu reagieren. Wenn wir (als Lehrende) unsere Studierenden dazu aufrufen, verantwortlich zu handeln, aber die Grenzen des Handlungsspielraums verschweigen, handeln wir selber unverantwortlich. Kaum ein Arbeitnehmer kennt die rechtlichen Grenzen der Treuepflicht – „viele Arbeitnehmer trauen sich auch bei erheblichen Missständen nicht, aktiv zu werden", andere ge-

fährden ihren Arbeitsplatz durch „unüberlegtes Offenbaren bedenklicher Verhaltensweisen des Arbeitgebers“ (Müller 2004).

Für die Fachdisziplin ist die Identifizierung struktureller Probleme essentiell, um diese kollektiv angehen zu können. Damit wird sie zum einen ihrer Verantwortung als Disziplin der Gesellschaft gegenüber gerecht und vergrößert zum anderen die Handlungsmöglichkeiten des Einzelnen.

Wir haben (in Bittner und Hornecker 2002) anhand einer historischen Rekonstruktion des Verantwortungsbegriffs (nach Bayertz 1995) gezeigt, wie ein entwickeltes begriffliches Instrumentarium hilft, das Verhältnis von Verantwortung und informatischer Praxis zu reflektieren. Um jemandem Verantwortung zuzuschreiben, muss diesem die Einsicht in die Folgen des Handelns möglich sein. Diese Einsicht wird bei IT-Fachkräften durch den enormen Zeitdruck sowie die Unkenntnis des Einsatzbereichs jedoch oft behindert. Zudem reduziert die in Unternehmen häufig noch vorherrschende Arbeitsteilung in Analyse und Implementierung die verfügbare Kontext-Information. Ohne Kontakt zu Anwendern und Betroffenen werden nur vorgegebene Anforderungen realisiert, die häufig nicht den tatsächlichen Problemen im Einsatz entsprechen. Negative Folgen von Designentscheidungen sind daher nicht absehbar und meist auch nicht intendiert. Vieles deutet darauf hin, dass es sich um ein systemisches Problem der Struktur der Organisation von Software-Entwicklung (SE) handelt (siehe u.a. Twisselmann 2000). Methoden des Partizipativen oder User-Centered Designs sind ein Schritt in die richtige Richtung, aber kein Allheilmittel.

Diese Einsicht bedeutet leider noch nicht, dass es alternative Handlungswege gibt: Die hochgradige Arbeitsteilung in der Software-Entwicklung begrenzt den Einflussbereich Einzelner, die rechtlich/vertraglich geforderte Loyalität zum Arbeitgeber schränkt den Handlungsraum weiter ein. Die Verantwortlichkeit für eine termingerechte Fertigstellung oder das Zurückhalten von Information kann dabei der Verantwortung für das Wohl eines Kunden entgegenstehen. Hier spielt wiederum die Unternehmenskultur eine große Rolle, die Prioritäten und Werte festlegt. Sie bestimmt, wer welche Handlungsspielräume hat und ob überhaupt (zumindest firmenintern) über moralische Konflikte offen gesprochen werden kann.

Schlusswort

Für notwendig halten wir aufgrund unserer Überlegungen, den Blick verstärkt auf die eigene informatische Praxis zu richten. Dies bedeutet u.E. zum einen die Begründung einer professionsorientierten Forschungsrichtung in der Informatik und zum anderen einen veränderten Ansatz zur Vermittlung von Ethik in der Lehre. Langfristig sollten wir eine Fachkultur etablieren, in der das Diskutieren über die eigene Berufspraxis und das Erzählen von *Geschichten* aus der Praxis sowie ihre Reflexion alltäglich sind.

Wir danken Marjo Rauhala (igw, TU Wien) für Diskussionen über die diesem Artikel zugrunde liegenden Gedanken.

1 *Whistleblower sind „Arbeitnehmer, die für sich das Recht der freien Rede in Anspruch nehmen und die Öffentlichkeit über bedenkliche oder rechtswidrige Praktiken ihres Arbeitgebers, eines Vorgesetzten oder anderer Arbeitnehmer informieren.“ (Müller 2004)*
„Whistlebolwing involves the deliberate disclosure of information about non-trivial activities which are believed to be dangerous, illegal, unethical, discriminatory or to otherwise involve wrongdoing, generally by current or former organisation members.“ (Hersh 2002)
Hersh 2002 gibt einen Überblick über den Forschungsstand zum Whistleblowing und kommt zu dem Schluss, dass es keine übereinstimmende Definition gibt. Verschiedene Autoren und Fachorganisationen erachten verschiedene Eigenschaften der Akteure (z.B. Art der Zugehörigkeit zu einer Organisation), der Adressaten (Arbeitgeber), der Situation (welches Risiko besteht, was wurde vor dem Whistleblowing versucht, welche Alternativen gibt es) und der Motive des Whistleblowers als zentral.

2 *Sarbanes-Oxley-Act SOX, 2002*

Literatur:

Bayertz, K. Eine kurze Geschichte der Verantwortung. In Bayertz, K. (Hrsg.): Verantwortung: Prinzip oder Problem? (S. 3-71) Darmstadt: Wissenschaftliche Buchgesellschaft 1995

Bittner, P.; Hornecker, E.: Responsibility and the Work of IT-Professionals. From Academia to Practice. In Brunnstein, K.; Berleur, J. (Hrsg.): Human Choice and Computers. (S. 171-181) Boston: Kluwer Academic Publishers 2002

Däubler, W.: Wann darf ein Arbeitnehmer 'Nein' sagen? FIfF-Kommunikation 4/2000, 29–31

Forester, J.F. (1999): The Deliberative Practitioner. Encouraging Participatory Planning Processes. Cambridge/London: MIT Press

Hanseth, O.; Monteiro E. (1994): Ethics versus Politics in System Development. Proc. IFIP WG 9.1 Workshop Ethics and Systems Design. The Politics of Social Responsibility, Havana, Cuba 1994 (Eds: Andrew Clement, Mike Robinson, Lucy Suchman, Ina Wagner) p. 51-56

Hersh, M.A. (2002): Whistleblowers – Heroes or Traitors? Individual and Collective Responsibility for Ethical Behaviour. Annual Reviews in Control Vol 26, 26(2), pp. 243-260. Elsevier

Hornecker, E.; Bittner, P.: Vom kritischen Verhältnis zur Berufspraxis in der Informatik – Ergebnisse einer Befragung. FIfF-Kommunikation 1/2000, 33–39

Kling, R. (1996): Beyond Outlaws, Hackers and Pirates. In Kling, R. (Hrsg.): Computerization and Controversy. (S. 848-869). 2nd ed.. San Diego: Academic Press

Lynch, W. T.; Kline, R. (2000): Engineering Practice and Engineering Ethics. Science, Technology and Human Values 25(2), 195–225

Müller, M. : Trendbegriff Whistleblower. Mitbestimmung 1+2/2004. S, 64-66

Twisselmann, Ute (2000): Informatik und Arbeitsumgebungen, FIfF-Kommunikation 1/2000, 28–31.