Indian Journal of Psychiatry, 2004, 46(2)99-103

Computer Ethics and Cyber Laws to Mental Health Professionals

Raveesh B N [*1], Sanjay Pande[2]

ABSTRACT

The explosive growth of computer and communications technology raises new legal and ethical challenges that reflect tensions between individual rights and societal needs. For instance, should cracking into a computer system be viewed as a petty prank, as trespassing, as theft, or as espionage? Should placing copyrighted material onto a public file server be treated as freedom of expression or as theft? Should ordinary communications be encrypted using codes that make it impossible for law-enforcement agencies to perform wiretaps? As we develop shared understandings and norms of behaviour, we are setting standards that will govern the information society for decades to come.

Key words: computer, cyber law and ethics

Introduction

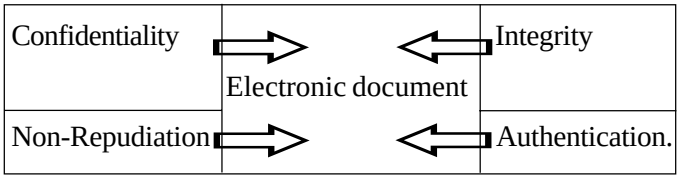
Computer is no longer the realm of computer specialist alone. Computer and information technology is developed and used in a social context rich with moral, cultural and political ideas. It is everywhere and for every individual. The uses are multi-dimensional. Today, every one of us is not only using computers but also, we have developed a pressing need for it. If one were driving a vehicle on a road, one would perhaps like to know (has to know) the laws of the place governing the road use. Similarly, one needs to know what are the laws applicable therein when computers are used.

The central task of computer ethics is to determine what we should do and what our policies should be. However, the reasons to study ethical issues surrounding computer and information technology is so fascinating that, one has to understand the environments in which it is being used. In this respect, the study of computer ethics turns out be the study of human beings (which is a mental health professionals core) and society- our goals and values, our norms of behaviour, the way we organize ourselves and assign rights and responsibilities. Ethical analysis precedes law when it is the basis for creation of a law, in this regard it becomes essential to consider ethical issues before one discusses about law (Maner, 1996).

One of the most salient concerns was that computers threatened our notion of what it means to be humans because computers could do the very thing that was considered unique to humans, rational thinking. There was much discussion of artificial intelligence. There was some fear (and fascination with the idea) that computers might take over decision making from humans. These concerns did not come from an effect arising from the use of computers but they arose from the mere idea of computers (Friedman, 1997). The very idea of a technology that could think or do something very close to it was threatening of what it means to be human. Ironically, it could be argued that this idea, that computers do what humans do, has turned out to be rich in its influence on human thinking about thinking rather than a threat. The model of human thought that computers provide has spawned the thriving new field of cognitive science and changed a number of related disciplines (Bynum and Terrell, 1993).

Computer ethics is a new branch of ethics that is growing and changing rapidly as computer technology also grows and develops. The term "computer ethics" is open to interpretations both broad and narrow. On the one hand, for example, computer ethics might be understood very narrowly as the efforts of professional philosophers to apply traditional ethical theories like Utilitarianism, Kantianism, or virtue ethics to issues regarding the use of computer technology. On the other hand, it is possible to construe computer ethics in a very broad way to include as well, standards of professional practice, codes of conduct, aspects of computer law, public policy, corporate ethics—even certain topics in the sociology and psychology of computing (Forester and perry, 1990).

Security in Electronic Transmissions.



[1]Assistant Professor, Dept. of Psychiatry, JSS Medical College & Hospital, Ramanuja Road, Mysore-04. e-mail : raveesh6@yahoo.com.

[2]Dept. of studies in Computer Science, University of Mysore, Manasa Gangotri, Mysore.

*Correspondence

What is Computer Ethics?

Moor's definition has been the most influential one. He defined computer ethics as a field concerned with "policy vacuums" and "conceptual muddles" regarding the social and ethical use of information technology. A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with new capabilities and these in turn give us new choices for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of computer ethics is to determine what we should do in such cases, that is, formulate policies to guide our actions. One difficulty is that along with a policy vacuum there is often a conceptual vacuum. Although a problem in computer ethics may seem clear initially, a little reflection reveals a conceptual muddle. What is needed in such cases is an analysis that provides a coherent conceptual framework within which to formulate a policy for action (Moor, 1985).

Computer ethics identifies and analyzes the impacts of information technology upon human values like health, wealth, opportunity, freedom, democracy, knowledge, privacy, security, self-fulfillment, and so on. This very broad view of computer ethics embraces applied ethics, sociology of computing, technology assessment, computer law, and related fields. It employs concepts, theories and methodologies from these and other relevant disciplines (Maner, 1996).

Computer Crime

In this era of computer "viruses" and international spying by "hackers" who are thousands of miles away, it is clear that computer security is a topic of concern in the field of computer ethics (Deborah, 1985). The problem is not so much the physical security of the hardware (protecting it from theft, fire, flood, etc.), but rather "logical security", which is divided into five aspects:

1. Privacy and confidentiality.
2. Integrity — assuring that data and programs are not modified without proper authority.
3. Unimpaired service.
4. Consistency — ensuring that the data and behavior we see today will be the same tomorrow.
5. Controlling access to resources.

Privacy and Anonymity

The ease and efficiency with which computers and computer networks can be used to gather, store, search, compare, retrieve and share personal information make computer technology especially threatening to anyone who wishes to keep various kinds of "sensitive" information (e.g., medical records) out of the public domain or out of the hands of those who are perceived as potential threats. During the past decade, commercialization and rapid growth of the internet, the rise of the world-wide-web, increasing "user-friendliness" and processing power of computers and decreasing costs of computer technology have led to new privacy issues, such as data-mining, data matching, recording of "click trails" on the web, and so on (Tavani, Herman and Moor, 2001).

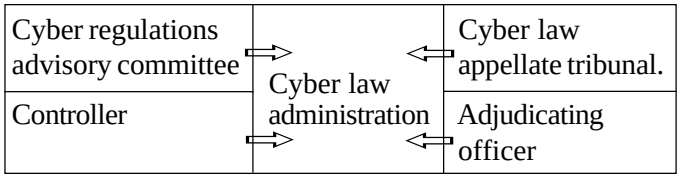
Questions of anonymity on the internet are sometimes discussed in the same context with questions of privacy and the internet, because anonymity can provide many of the same benefits as privacy. For example, if someone is using the internet to obtain medical or psychological counseling, or to discuss sensitive topics (for example, AIDS, abortion, gay rights, venereal disease, political dissent), anonymity can afford protection similar to that of privacy (Introna, 1997). Similarly, both anonymity and privacy on the internet can be helpful in preserving human values such as security, mental health, self-fulfillment and peace of mind. Unfortunately, privacy and anonymity also can be exploited to facilitate unwanted and undesirable computer-aided activities in cyberspace, such as money laundering, drug trading, terrorism, or preying upon the vulnerable (Nissenbaum, 1999).

THE INFORMATION TECHNOLOGY ACT, 2000

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto (Bare Act, 2000).

Some of the salient sections relevant to mental health professional are Section 4, Legal recognition of electronic records and Section 5, Legal recognition of digital signatures.

Cyber law administration structure
(Ministry of information technology, Government of India).



PENALTIES AND ADJUDICATION

Section 43, Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, —

(a) Accesses or secures access to such computer, computer system or computer network;

(b) Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees, to the person so affected.

THE CYBER REGULATIONS APPELLATE TRIBUNAL

Section 48, Establishment of Cyber Appellate Tribunal.

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in subsection (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Section 57, Appeal to Cyber Appellate Tribunal.

(1) Same as provided in sub-section (2), any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of twenty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of twenty -five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

Section 59, Right to legal representation.

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

Section 61, Civil court not to have jurisdiction.

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Section 62, Appeal to High Court.

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

OFFENCES

Section 65, Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Section 66, Hacking with computer system.

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

Section 67, Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Section 71, Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from, the controller or the certifying authority for obtaining any licence or Digital Signature Certificate, as the case may be. shall be punished with imprisonment for a term, which may extend to two years, or with fine, which may extend to one lakh rupees, or with both.

Section 72, Penalty for breach of confidentiality and privacy.

Same as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 74, Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment

for a term, which may extend to two years, or with fine, which may extend to one lakh rupees, or with both.

Section 75, Act to apply for offence or contravention committed outside India.

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Section 76, Confiscation.

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation, provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Recommendations

1. The new mental health legislation should make provision to describe the policy of information technology in the field of mental health in India.
2. To develop the international consensus as to where cyber crimes fall with regard to the issue of diagnosis and classification.
3. To develop more knowledge base from psychiatric perspective on epidemiology of computer and cyber related morbidities.
4. There is a need to include the topic on relationship of information technology and mental health at postgraduate level (to begin with).
5. Integrating IT and mental health professionals to initiate and improve clinical and research activity.

Conclusion

Information technology (computer and cyber/internet) has begun to affect (in both good and bad ways) community life, family life, human relationships, education, freedom, democracy, and so on. Computer ethics in the broadest sense can be understood as that branch of applied ethics which studies and analyzes such social and ethical impacts of information technology. In recent years, this robust new field has led to new university courses, conferences, workshops, professional organizations, curriculum materials, books, articles, journals, and research centers. And in the age of the world-wide-web, computer ethics is quickly being transformed into “global information ethics”. Thus, making every citizen in general and various professionals in particular to know about the ethical and legal issues intricated.

References

Bynum and Terrell W(1993). “Computer Ethics in the Computer Science Curriculum.” In Bynum, Terrell Ward, Walter Maner and John L. Fodor, eds. (1993) Teaching Computer Ethics, Research Center on Computing & Society.

Deborah G J (1985). Computer Ethics, Prentice-Hall, 2nd Edition, 1994.

Forester, T and Perry M(1990). Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, MIT Press.

Friedman, B(1997). Human Values and the Design of Computer Technology, Cambridge University Press.

Introna, L D(1997).”Privacy and the Computer: Why We Need Privacy in the Information Society,” Metaphilosophy, Vol. 28, No. 3, 259-275.

Maner, W(1996). “Unique Ethical Problems in Information Technology,” In Bynum and Rogerson. (1996) 137-52.

Moor, J H (1985). “What Is Computer Ethics?” In Bynum, Terrell Ward, ed. (1985) Computers and Ethics, Blackwell, 266-75.

Nissenbaum, H(1999).”The Meaning of Anonymity in an Information Age,” The Information Society, Vol. 15, 141-144.

Tavani, Herman T. and Moor J H (2001). “Privacy Protection, Control of Information, and Privacy-Enhancing Technologies”, Computers and Society, Vol. 31, No. 1, 6-11.

The Information Technology Act, (2000). Bare Act, Gazette of India, Government press, N Delhi.