Appendix II

Esteemed Respondent,
(Note:- Rest assured your identity and Information collected from yougoodself would be kept confidential.)

Regulation of cyber space: A socio-legal study with special reference to cyber law in India
(Rest assured all the information provided herein by the respondents viz personal biodata, responses, views and suggestions, etc. will be kept strictly confidential and entire gammit of information will be solely utilized only and only for research, analysis and academic purposes with utmost precaution).

Questionnaire for Law students
This questionnaire is designed to get your views on your awareness, knowledge and attitude towards Regulation of cyber space with special reference to cyber law in India and is divided into 4 sections containing a total of 37 Questions and suggestion. In case you do not understand any question, please feel free to ask and get doubts clarified. Kindly fill all columns at your best and don’t leave any question unanswered in the interest of this research endeavour.

Section 1: Demographic Data ( fill / tick the columns properly and correctly to the best of your knowledge).
1. Name: ________________________________
2. Class: __________________ Semester/ Year: __________________
3. Age: _____ Years _______ Months
4. Gender : Male / Female
5. Religion: Hindu / Sikh / Muslim /Christian / Parsi / any other
6. State to which you belong: __________________ Mother Tongue ________
7. Region: Rural/ Urban
8. Are you Computer Literate Yes/ No
9. E mail address:- If any, ________________________________
(Point 9 is only for the sake of any clarification, etc.).

Section 2: Awareness about Cyberspace and need for its regulation and control.
10. Are you aware that Cyberspace describes the world of space of computers and the society that gathers around them: Yes / No / NR
11. Are you using cyberspace through internet : Yes / No / NR
12. If yes, how many hours do you spend in cyberspace (using internet) in
   I) a day: ________, II) in a week ________, III) in a Month ________
13. Do you have internet connection

Yes / No

14. If Yes, what is your mode to access Internet :-

1) Computer ______________________
2) Mobile ______________________
3) Any other (Please Specify) ______________________

15. If no, what is your other source for internet access:-

1) Cyber Café ______________________
2) Library ______________________
3) Any other (Please Specify) ______________________

16. Have you taken Digital Signatures to certify your document in cyberspace? Yes / No / NR

17. For what purposes you are using cyberspace(through internet) Information:

a. Communication with govt. Yes / No
b. Land records Yes / No
c. Complaints Yes / No
d. Business Work Yes / No
e. Pursuit of Education/ Knowledge Yes / No
f. Chatting/Social Networking Yes / No
g. Banking Yes / No
h. Health Care Yes / No
i. Face Book Yes / No
j. If any other purpose (Pl. Specify) ______________________

18. Are you aware about cyber crimes: Yes / No / NR

19. Have you come across any cyber crime during use of cyberspace through internet: Yes / No / NR

20. If you feel comfortable you may specify/describe the cyber crime you came across :-

______________________________
______________________________
______________________________

Section 3: Knowledge about Cyberspace and its regulation
Appendix II

21. Does the term cyberspace was originally coined by William Gibson in his short story *Burning chrome:* Yes / No / NR

22. Do you agree that Cyberspace is a virtual space, which is unconstrained by geographic boundaries. Yes / No / NR

23. Does Cyber law mean norms, ethics, rules and regulations, etc. which are essential to create system/discipline and orderly control, etc., in cyberspace. Yes / No / NR

24. Is India amongst few of the countries, which have any legal framework for e-commerce and e-governance? Yes / No / NR

25. Do you think that the Information Technology Act, 2000 of India is a comprehensive piece of legislation, which aims at policing and regulating all the activities in the cyberspace. Yes / No / NR

26. Is it correct that The Information Technology Act, 2000 of India consists of 15 Chapters and 90 Sections? Yes / No / NR

27. Does The Information Technology Act, 2000 provides for a particular technology (viz asymmetric crypto system and hash function) as a means of authenticating electronic record. Yes / No / NR

28. Does The Information Technology Act, 2000 also applies to documents mentioned in First Schedule such as Negotiable Instrument, Power of Attorney, Trust, etc. Yes / No / NR

29. Is it correct that “The Information Technology Act, 2000” been amended by The Information Technology (Amendment ) Act 2008? Yes / No / NR

30. Does “The Information Technology Act, 2000” provides for cross border Taxation policy? Yes / No / NR

Section 4: Opinion and Attitude towards Cyberspace and its regulations and control, etc.
(Note :- Please tick mark one best option between A to E for all the seven categories detailed below from A to G.)
31. Cyberspace can be successfully used for carrying out following human activities:

<table>
<thead>
<tr>
<th>S. no</th>
<th>Caption Connection</th>
<th>Strongly Agree A</th>
<th>Agree B</th>
<th>No Comment C</th>
<th>Disagree D</th>
<th>Strongly Disagree E</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Communication (in the form of e-mails, chatting, conferencing and creating face book, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Seeking Information (inform of websites)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>For Education (e-learning), etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>For Health (e-health)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>For Banking (e-banking)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>For Commerce (e-commerce, advertising), etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>For Governance (e-governance)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

32. Cyberspace can be viscously used for carrying out following criminal activities:

(Nota :- Please tick mark one best option out of five choices from A to E for all the eight caption connection categories (A to H) detailed horizontally.)

<table>
<thead>
<tr>
<th>S. no</th>
<th>Caption Connection</th>
<th>Strongly Agree A</th>
<th>Agree B</th>
<th>No Comment C</th>
<th>Disagree D</th>
<th>Strongly Disagree E</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Computer-Related Crimes, etc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Communications in Furtherance of Criminal Conspiracies, etc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>For Infringement of Intellectual Property Rights, Infringement of human rights, etc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>For Dissemination of Offensive Materials, etc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix II

E For Electronic Money Laundering and Tax Evasion, defrauding, etc

F For Electronic Vandalism, Terrorism & other disastrous, nefarious activities, etc.

G For Sales and Investment Frauds, etc.

H Infringement of Right to Privacy viz Paparazzi, Obscenity, etc.

<table>
<thead>
<tr>
<th>S.no</th>
<th>Caption Connection</th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>No Comment</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>Cyberspace has increasingly become integrated into virtually every aspect of social living in some form or the other.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ii</td>
<td>Cyberspace is a double edge sword, which can be used for constructive as well as destructive activities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iii</td>
<td>Cyberspace needs to be regulated in India parallel to advanced countries, like U.S.A., U.K., Japan, etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iv</td>
<td>Cyberspace can be regulated using, legal controls such as rules, regulations, acts etc. for healthy and all round development of people of India</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>Cyberspace can be self-regulated by the social norms of customs, etc. whatever community one chooses to associate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vi</td>
<td>Cyberspace can be regulated using</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

33. Please give your opinion about regulation of cyberspace i.e. how cyberspace can be regulated? Please tick-mark only one of your best choice) spread in five options (A to E) for each following ten caption connection categories from I to X.
<table>
<thead>
<tr>
<th>Q</th>
<th>Question</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>vii</td>
<td>The Information technology Act has established legal certainty, legal axis for cyberspace users.</td>
<td></td>
</tr>
<tr>
<td>viii</td>
<td>There is need to amend Information technology Act so as to further plug and reduce legal uncertainties, infirmities, flaws in cyberspace</td>
<td></td>
</tr>
<tr>
<td>ix</td>
<td>The biggest challenge before Cyber Law is its integration with the legacy system of laws applicable to the physical world</td>
<td></td>
</tr>
<tr>
<td>x</td>
<td>There is need to spread Awareness regarding these cyber laws among the masses</td>
<td></td>
</tr>
</tbody>
</table>

34. Is Present legislation sufficient and successful in regulating cyberspace? **Yes / No / NR.**

35. Does we need new laws for better regulation of cyberspace? **Yes / No / NR.**
   If yes, kindly give your suggestions.

36. Please give your valuable suggestions if any as to how to regulate cyberspace in India in a better way.

   ____________________________________________________________________________

   ____________________________________________________________________________

   ____________________________________________________________________________

   ____________________________________________________________________________

   ____________________________________________________________________________

   ____________________________________________________________________________

   ____________________________________________________________________________

   (Signature of the Respondent)

   **Thanks for your kind Cooperation**

   **(Researcher)**
Certificate of Presentation in National Conference

LAW AS A FACILITATOR OF SOCIO-ECONOMIC REFORMS IN THE PRESENT DECADE

Organised by Panjab University, Chandigarh
March 27th - 28th

This is to certify that Prof. Dr. (Ms. Mr.) Akshat Khurana (co-author) presented a paper on "Regulation of Cyber-Space with Special Reference to the Reforms in the Present Decade" in the All India Law Congress - 2010 on "Law as a Facilitator of Socio-Economic Reforms in the Present Decade" held in Panjab University, Chandigarh.

Director

Organising Secretary

VII
Regulation of cyber space with special reference to The Information Technology (Amendment) Act, 2008

Akash Khosla, Meenu Paul
Department of Laws, Panjab University, Chandigarh

Abstract:
Cyber activity has become an essential part of the general public’s everyday life. Virtually every aspect of our society is becoming linked to cyberspace, from civilian, government, and the military, to public utilities, communications, transportation, and financial systems. Unregulated cyber space is a major threat to national security and economy. It heads the society towards a social damage. India is amongst few of the countries in the world which have any legal framework for e-commerce and e-governance. Information Technology Act, 2000 (IT Act, 2000) was enacted for this purpose which consisted of 94 sections segregated into 13 chapters. Four schedules formed part of the Act. It chiefly covered: E-commerce in India, (b) E-governance in India, (c) Cyber contraventions and (d) Cyber crimes. The Government of India has brought major amendments to ITAct-2000 in form of the Information Technology Amendment Act, 2008. The amended act provides additional focus on Information Security. It has added several new sections on offences including Cyber Terrorism and Data Protection. However amendments are found to be largely inadequate and far behind in time. It has been realized that this act is not the end but only beginning of to a plethora of legislation that still needs to be formed. There is need to implement the legal reform agenda and emphasis is to be placed on social regulation and governance.
Appendix III

Introduction

"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding." -

William Gibson, 1984

Cyberspace is an online forum utilizing advanced technology to provide interactions with others. Different authors have defined cyberspace in different ways. Webster’s Collegiate Dictionary defines Cyberspace as an "online world of computer networks." Randell Farmer (1989) explained his idea of Cyberspace as "...a place, not just an interface or a metaphor. A place where people, regardless of location, hardware, or purpose can get together in a participatory experience to conduct business, socialize, or have a good game-----." Bauwens (1994) suggests that “Cyberspace is a place we are in when we are involved in computer-mediated communications”. Roberts, Smith and Pollock (1996) contend that Cyberspace is the "location of mediated interactions in unspecified environments."

The term "Cyberspace" often brings with it connotations of an imaginary world, a non-world, a simulated or unrealized space. Disregarding the conceptual idea of Cyberspace, however, one realizes an authentic, perceptual space made up of computer bases, hardware, modems, telephone lines, electrical lines, satellite stations and human beings (Strate, 1999). Within these tangible elements lie the components for a sense of space generated within the mind, a dimension we call Cyberspace.

Cyber activity has become an essential part of the general public’s everyday life. It has become integrated into virtually every aspect of social living. There are few human activities that do not involve the use of cyberspace in some form or other. E-commerce, e-business, e-education, e-health, telemedicine, e-mail, e-governance, e-banking, e-ticketing, e-contract etc., are some of the useful applications of cyberspace. Banking, stock exchanges, air traffic control, telephones, electric power, and a wide range of institutions of health, welfare, and education are largely dependent on information technology and telecommunications for their operation.
Today, computers have become essential to the transacting of our nation's daily business. Everything from telephones to transportation, power networks, our financial system, emergency services, and our national defense depends upon computers. Together, these components, networks, and systems make up the national information infrastructure. Now, more than ever, our military and other critical government personnel rely upon these networks and systems to maintain our national security. Virtually every aspect of our society is becoming linked to cyberspace, from civilian, government, and the military, to public utilities, communications, transportation, and financial systems. These links are creating vast efficiencies in the delivery of goods and services and giving people throughout the world greater access to information and ideas.

Need for regulation
Phenomenal growth in the use of Cyberspace in almost every walk of life has posed the challenge of regulating the cyberspace. The Cyberspace is an open system where heterogeneous agents can appear and disappear unpredictably. As the number of agents on the Cyberspace increases, there is a need to regulate services and content of Cyberspace. Cyberspace calls into question many traditional legal conceptions like ownership, freedom of expression, liability, property etc. Incidents involving break-ins to computer systems causing disruption of service, destruction, and alteration of data have happened and appear to be rising at a disturbing rate. Cyberspace permits anonymity and pseudo anonymity. Users can mask their real flesh and blood identities and assume digital avatars. Anonymous remailers facilitate sending messages without revealing their identity or origin. Cyber crime is the latest and perhaps the most complicated problem in the Cyberspace.

Cyber crime includes any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes. A generalized definition of cyber crime may be “unlawful acts wherein the computer is either a tool or target or both”. The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking etc. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data diddling, salami attacks, logic bombs, trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.
The variety of criminal activity which can be committed with or against information systems is surprisingly diverse. Some of these are not really new in substance; only the medium is new. Others represent new forms of illegality altogether. Some of the frequently observed cyber crimes are:-

a) Theft of information services  
b) Communications in furtherance of criminal conspiracies  
c) Telecommunications piracy  
d) Dissemination of offensive materials  
e) Electronic money laundering and tax evasion  
f) Electronic vandalism and terrorism  
g) Sales and investment fraud  
h) Illegal interception of telecommunications  
i) Electronic funds transfer fraud  
j) E-mail online spams  
k) Email spoofing  
l) Email bombing  
m) Destruction of digital information through use of viruses  
n) IPR violations  
o) Fraudulent online investment newsletters  
p) Sale of illegal articles  
q) Breach of privacy and confidentiality

Hart in his work “The Concept of Law” has said ‘human beings are vulnerable so rule of law is required to protect them’. Applying same principle to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. Therefore India has enacted the “Information Technology Act, 2000”. It is a comprehensive piece of legislation which aims at policing some of the activities over the Internet.

**Information Technology Act, 2000**

Information Technology Act, 2000 is an Act, “To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred as “electronic commerce”, which involved 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 Banker’s Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto”.

Salient features of the Act
The salient features of the Information Technology Act, 2000 are as follows:—
(i) Extends to the whole of India (Section 1)
(ii) It provides for authentication of electronic records (Section 3)
(iii) It gives legal framework for affixing Digital signature by use of asymmetric crypto system and hash function (Section 3)
(iv) It gives legal recognition of electronic records (Section 4) and electronic signatures (Section 5)
(v) It provides for retention of electronic record (Section 7) and publication of Official Gazette in electronic form (Section 8)
(vi) It gives security procedure for electronic records and digital signature (Sections 14, 15, 16)
(vii) It provides for licensing and regulation of Certifying authorities for issuing digital signature certificates (Sections 17-42)
(viii) It defines functions of Controller (Section 18) and gives recognition of foreign Certifying Authorities (Section 19)
(ix) It provides for Data Protection (Sections 43 & 66)
(x) It define various types of computer crimes and provides for stringent penalties (Section 43 and Sections 66, 67, 72)
(xi) It provides for appointment of Adjudicating officer for holding inquiries under the Act (Sections 46 & 47) and establishment of Cyber Appellate Tribunal under the Act (Sections 48-56)
(xi) The provisions of the Act also apply for offences or contraventions committed outside India (Section 75)
(xii) The Act gives power to police officers and other officers to enter into any public place and search and arrest without warrant (Section 80)
(xiii) It provides for constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller (Section 88)
Strength of amended Information Technology Act, 2000

The Information technology Act 2000 has been substantially amended through the Information Technology Amendment Act 2008 which was passed by the two houses of the Indian Parliament on December 23 and 24, 2008. It got the Presidential assent on February 5, 2009 and was notified for effectiveness on October 27, 2009. Some of the important amendments are:-

- Some new definitions has been added:-

  A new section has been inserted to define “communication device” to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.

  A new section has been added to define “cyber café” as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.

  A new definition has been inserted for “intermediary”. “Intermediary” with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

- New Section included to address electronic contract (Section 10A), data protection and privacy (Section 43).

- It necessitate body corporate to implement best security practices (Sections 43A & 72A).

- The single member Appellate Tribunal has been changed to multimember (Sections 49-52).

- New Section added to address new forms of computer misuse (Section 66-67).

- It provides for preservation and retention of Data/Information (Section 67C).

- Existing Section 69 has been revised to empower Central Government to designate agencies and issue direction for interception and safeguards for monitoring and decryption.
Appendix III

- It provides for blocking of Information for public access under certain circumstances (Section 69A).
- New section added for designating agency for protection of Critical Information Infrastructure (Section 70A).
- New Section to provide power to CERT to call and analyse information relating to breach in cyber space and cyber security (Section 70B).
- Revision of existing Section 79 for prescribing liabilities of service providers in certain cases and to empower Central Government to prescribe guidelines to be observed by the service providers for providing services.
- New Section added which provides for Examiner of Digital Evidence (Section 79A)

Weaknesses of amended Information Technology Act, 2000

There has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The amendments have been criticized on basis of a large number of pitfalls such as:-

a) Proper procedure not followed

The amendment was passed in an eventful Parliamentary session on 23rd of December 2008 with no discussion in the House.

b) Inadequate provisions-

i) Inadequacy in providing sufficient data protection provisions-

India has neither learnt from the wisdom of the United States nor the European Union, in terms of their respective experiences, in the area of data protection. The provisions does not aid the victim entities, whose data and information is often misused by their employees or agents with impunity.

ii) The IT Act does not offer much in terms of protection of intellectual property on the net. In other words there are no provisions in the act to protect copyrights, patents or trademarks.

iii) There is lack of legal and procedural safeguards to prevent violation of civil liberties of Indians. On privacy issues also the Act has come in for a lot of flak.
Appendix III

C) Reduction in deterrent effect.

i) The older version of IT Act 2000 has provided for punishment for various cyber offences ranging from three years to ten years. These were non-bailable offences where the accused was not entitled to bail as a matter of right. However, the amendments to the IT Act have gone ahead and reduced the quantum of punishment and made many offences bailable. For instance the quantum of punishment on first conviction for publishing, transmitting or causing to be published any information in the electronic form, which is lascivious, was five years which has been reduced to three years.

ii) Similarly, the quantum of punishment for the offence of failure to comply with the directions of the Controller of Certifying Authorities has been reduced from three years to two years.

A careful analysis of the said amendments, clearly bring home the point that the new amendments are not at all sufficient in the context of emergent needs of corporate India and have various glaring loopholes. The expectations of the nation for effectively tackling cyber crime and stringently punishing cyber criminals have all been let down by the extremely liberal amendments, given their soft corner and indulgence for cyber criminals. All in all, given the glaring loopholes as detailed above, the new IT Act amendments are likely to impact adversely the regulation of cyberspace.

Conclusions and Suggestions

The existence of cyberspace as a new operational realm presents us with new opportunities for its employment and vulnerabilities to be defended against, as discussed previously, and its capabilities challenge the strategist to integrate those capabilities with other elements and instruments of power. The march of technology demands the enactment of newer legislation both to regulate the technology and also to facilitate its growth. The Indian legal system though robust and based on a strong historical tradition is proving somewhat ineffective for the growth and development of advancing technologies. There is need of enhancing legal research, awareness and capacity building measures for increasing manpower in the field of cyberspace regulation. The law pertaining to regulation of cyberspace should be self-containing and easily comprehensible to the global village community. The formulation of an International Model Law on Cyber crime (based on
which various countries could legislate and ensure harmony between various territorial
laws) could be one of the more practical approaches.

In conclusion, it is not possible to eliminate cyber crime from the cyber space. However, it is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime. There is need to implement the legal reform agenda.

References

a) Cyber Crime by Parthasarathi Pati
b) Cyber crime and information warfare by Dr Peter Grabosky
c) Economic Times, Chandigarh dt. 25 June 2007, Pg.3
d) The new Information Technology Act Amendments by Pavan Duggal.
e) http://www.cert-in.org.in
Law Bhawan, Sector 37-A, Chandigarh.

&

INTERNATIONAL COUNCIL OF JURISTS

CERTIFICATE

Awarded to Mr./Ms. Akash Khasla

for

Presenting the papers on the topic The Use of Internet by Courts & the Judiciary in India

in the International Conference of Jurists on Judicial Reforms held on 13th March, 2010 at Panchkula

and 14th March, 2010 at Chandigarh (India).

PARTAP SINGH
Chairman
Bar Council of Punjab & Haryana

RAJEEV KASWAN
Hony Secretary
Bar Council of Punjab & Haryana
The Use of the Internet by Courts and the Judiciary in India

A. Khosla, M. Paul.
Deptt. of Laws, Panjab University, Chandigarh

Abstract:
The Information technology industry is growing at dazzling and dizzy speed. Its technical power seems to be increasing almost exponentially, its commercial base broadening at an astonishing rate, and its penetration in society and individual lives appears to be almost total. Electronic justice is use of information and communication technologies (ICT) in Judicial system. Use of ICT in justice system primarily helps in increasing administrative efficiency and access. Integration and automation of court procedures creates accountability and transparency in the judicial processes. Further, the timeliness can be drastically improved. Besides, Internet offers potential opportunities to deliver information, advisory, legal, and judicial services online and thereby help to increase the legitimacy. Above and beyond, the confidence of the public in the judicial system can be improved a lot by implementing e-justice, while achieving economic and social objectives of the country. Despite its potential use, e-justice implementation is a massive challenge for several nations like India as social and economic hindrances come in the way of e-justice.
Introduction

Technological Developments in the field of information and introduction of computers have made a turning point in the history of human civilization. It has brought about a sea change in all fields of human activity. It has resulted in enhanced efficiency, productivity and quality of output in every walk of life. Computers as well as electronic communication devices such as facsimile machines, electronic mail, video conferencing, provide the ability to process large volumes of data both with speed and accuracy. Moreover improved technology has enhanced exchange of useful information between different locations and support higher quality of decision making. These capabilities have contributed to more efficient and responsive systems not only in business organizations, but also in legal, governmental and other public systems. There has been considerable interest in recent years in the implementation of technology in the Court environments. Numerous jurisdictions including Australia, Singapore, Canada, United States and several others within Europe have made significant use of technology. Therefore understanding of the benefits of the use of information and communication technologies (ICTs) in courts and to make it judicially applicable for the deliverance of justice appropriately is essential for the Indian legal system and is in the larger public interest also.

Applications of Technology in dissemination of justice

Information technology can prove to be a boon in the process of dissemination of justice. The areas in which information technology would be of immense use may be broadly classified as follows:-

a) Case management
b) Public services
c) Courtroom and chamber proceedings
d) Judicial decision support
e) Judicial administration etc., etc.

Case management

With the advent of technology, new-age case management systems leverage on document imaging, electronic filing and automated workflow technology can be developed for
streamlining the process of case disposal. The launching of the Electronic Filing System (EFS) may provide four main services: the electronic filing service, electronic extract service, electronic service of documents and the electronic information service. Case management systems can revolutionize the whole process, from registration to disposal of cases, bringing the courts a step closer to the vision of a paperless court.

Public services

Information Technology can offer a plethora of ways in which public access to court services can be enhanced. The technologies, can enable the delivery of virtual court services, include: multimedia kiosks, Internet and intelligent voice response systems etc.. These can enhance public access to justice which is a primary concern of all judiciaries.

Courtroom and chamber proceedings

ICT can be used to streamline the procedures in courtrooms and also in chamber proceedings. Video conferencing provides a convenient means of communication between persons in different locations. It can be used for performing a number of tasks expeditiously in courtroom and chamber proceedings such as:-

a) For taking testimony of Witnesses,
b) Bail Video Link,
c) Remote Chamber Hearings,
d) Remote Hearings and Consultations,
e) Remote Interpretation Services,
f) International Co-mediation

Some of the benefits of using ICT in courtroom and chamber proceedings are:-

a) Dreaded criminals can be tried without risk
b) Trial is expedited with use of this facility
c) High Cost and manpower wastage in producing undertrials only for remand extension can be saved
d) Multiple trials of an accused lodged in one jail is possible in different states
e) Evidence of witnesses unable to come to Court can be recorded
Appendix III

f) In child sexual offences, minor witnesses can be screened from the accused by use of this facility

g) Accurate record of evidence takes place

h) Visual animations & presentation of Arguments

i) Real time monitoring of cases becomes more plausible.

j) Congenial and comfortable atmosphere increases efficiency, etc.

Judicial Decision Support

In the quest to dispense justice expeditiously in accordance with the law, the quality of Judicial decisions is fundamental. Therefore, computer technology which support judicial decision-making can enhance efficiency in the administration of justice. Record of Court can be stored on few DVDs. Judges can access a CD-ROM library for legal materials which increases awareness and help them in their decision making. Immediate retrieval of record has become possible with ICT. Internet aids are also available for citations as well as research work.

Use of Technology in the Indian Courts

Information technology is increasingly being used in Indian legal system for dissemination of justice. The 121st Report of the Law Commission of India (July 1987) has devoted a whole chapter to "Technological Advances and its use in the context of Judicial appointments". A beginning has been made by National Informatics Centre (NIC) in computerisation of Court records. The administrative system in the Supreme Court has been computerised. A query system allows litigants anywhere in the country to enquire and obtain information on the status of cases filed in the Supreme Court through NICNET. It is increasingly being used to track and manage the progress of the proceedings. Now input into the computer system of case number or the names of the parties provides the relevant key details of the case, such as the case number, parties’ name, name of solicitors, case type, stage of the case, outcome of the hearing etc. The case management systems are providing tools to the court staff to carry out many routine operational tasks more quickly and efficiently.
The Supreme Court is also introducing a Classification System as well as a system to track progress of cases and Case Flow System. Likewise the Gujarat High Court has also introduced a comprehensive case management system. Such systems are being initiated at other high courts too. ICT is increasingly being used for maintaining transparency in dissemination of justice. Both the Supreme Court and the High Courts have informational websites which provide historical background and the organisation structure of the Courts. The Supreme Court website also contains the weekly legal notices and hearing lists and speeches delivered by the Honourable Chief Justice of India. Video conferencing is becoming increasingly pervasive, its growth fueled by improved technology, lower cost, and the industry adopting open standards. Video conferencing should be used extensively in the Indian Judiciary. It needs to be ensured that video conferencing facilities are used to allow vulnerable witnesses to give evidence away from the court room, thereby saving these witnesses from any emotional trauma they may otherwise suffer in having to appear in court together with the aggressors.

E-courts in India are at the initial stage of establishment. All the court rooms in the Supreme Court and an increasing number of court rooms in the Subordinate Courts are being equipped with microphones and audio recorders to record the proceedings in courts. Digital recordings are also currently being studied. Till now India has done a good job by “computerising” the courts all over India. The next stage is to make effective use of Information and Communication Technology (ICT) for filing, contesting and adjudication of both civil and criminal disputes and litigations. The more important part to bring about a success in the use of technology in the courts is to bring out a change in the mindset of the judges, court administrators, lawyers and the litigants. Both judges and support staff should be imparted intensive training in information technology to adequately reap the benefits of ICT in Indian legal system.

**Conclusion**

Thus the Indian Judiciary (comprising both the Supreme Court and the Subordinate Courts) has been exploiting, intensively and extensively, the benefits of information technology in many aspects of its internal administration and operational processes. It is also actively encouraging
and promoting the use of information technology in the trial processes. But much deserves to be done to enhance the use of information technology in courts. Indian legal system needs to have a strategic vision to further reap the significant benefits of information and communication technology for Courts, users of the Courts and the community at large. We should study systems of advanced countries like U.S.A., U.K., France, Japan, etc. and make use of their experiences while modernizing our Indian legal system.

References:-

6. Singh TS. ICT in the district courts of Delhi- Challenges, strategies and solutions. Article available on line.
7. Upadhyay AC. Information technology and its impact on judiciary. Article available on line.