

Cyberlaws in Information Age

Asia-Pacific Regional Workshop on Equal Access of Women in ICT
Seoul, R.O.Korea, Oct. 22-26 2001

M. Ajmal Edappagath
Advocate
Supreme Court
India

1. Introduction

Information society geared by development and convergence of computer, telecommunication and broadcasting technologies – called, information and communication technologies (ICTs) – today destructively as well as creatively shifts paradigms of industries and life styles in many countries. Despite economic recessions are deepening globally at the dawn of 21st Century, consumer expenditures and industrial performances are still growing in the ICT sectors especially in the advent of Internet and its application like e-commerce. For instance, e-commerce sales alone estimated in 2003 –5 are about US\$ 1,000 billion compared to US \$ 26 billion in 1996-97.

There has been in tradition legislation designed to regulate various aspects of human activities. It used to be relatively easy for legislators to enact laws when a particular area of human activity needs to be regulated. Now, with the revolution of ICTs, it is not new activities *per se* but ways that people conduct their activities need to be regulated. Indeed, the ways of conducting human activities have substantially changed with the advent of technological revolution especially in the information or cyber era.

The technological revolution in the information and communication sectors in particular led the existing legislation to be ineffective to meet the new phenomena of human activities, especially in the areas where crimes are committed on and through the net.

Taking this wonderful opportunity, I would like to explore some emerging questions concerning cyberlaw as follows: e.g.,

- What is cyberlaw ?
- What are the main legal issues in cyber era ?
- What kind of legislation may be required against cybercrimes ?
- What is the scope of cyberlaw in case of India ?
- Whether are there any gender-sensitive cyberlaw ?; and last but not least,
- Legislative ways forward against cybercrimes ?

2. What is cyberlaw ?

Most people think of Internet as being synonymous with the World Wide Web but it is not. The Internet is a network of computer networks. The very name Internet comes from the concept of inter-networking, where multiple computer networks are joined together. In the

business arena, electronic mail (e-mail), file transfer, and chat rooms take place through the World Wide Web. Together, they comprise a world of cyberspace, where important legal issues - i.e., cybercrimes - have been already raised.

The term 'cyberlaw' in general refers to all the legal and regulatory aspects of Internet. It means that anything concerned with, related to, or emanating from any legal aspects or issues concerning any activity of netizens and others in cyberspace comes within the ambit of cyberlaw.

More specifically, cyberlaw can be defined as a law governing the use of computer and the Internet. Namely, it focuses on a combination of state and federal statutory, decisional and administrative laws arising out of the use of Internet.

A fundamental question is 'whether and to what extent particular forms of conduct might be regarded as criminal under existing legal formulations'¹. The problem lies not in the fact that so many diverse kinds of crimes can be committed using the ICT – i.e., Internet, but the fact that the existing criminal law might be ill equipped to deal with this 'upgradation' in the methods and media of committing crimes. This challenge is posed due to two fundamental aspects: one is the relatively young age of the Internet and the corresponding antiquity of the present laws in force. The other is the irrelevance of geography, which poses serious questions with regard to jurisdictional matters that are fundamental for any criminal proceeding to take place."²

In accordance with the Computer Misuse Act (1990), the UK, the scope of new crimes or offences is defined in such cases as: e.g.,

- renders criminal any attempt to obtain unauthorized access to programs or data held on a computer;
- applies in the situation where the contents of a computer system are subjected to an unauthorized modification;
- attempts to deal with another aspect of computer related behavior, namely the speed with which conduct can move from preparation to perpetration.

In case of India, the Information Technology Bill³ (1999) has defined the cybercrimes as:

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

¹ Ian J. Lloyd & Moira J.Simpson, 'Computer Crime', Chris Reed (edited), *Computer Law*, Third Edition, 1996, Universal Law Publishing co., pp.241-274.

² Refer to "ICT Laws", which is one of e-learning modules on policy & regulation developed jointly by the ITU and OFTA in Hong Kong: [Http://www.itu-coe.ofta.gov.hk](http://www.itu-coe.ofta.gov.hk).

³ The Indian Government, *The Information Technology Bill*, 1999: [Http://www.mit.gov.in/it-bill.htm](http://www.mit.gov.in/it-bill.htm)., Nandan Kamath, *Law relating to Computers, Internet and E-commerce: A guide to Cyberlaws*, 2000, Universal Law Publishing Co. Pvt. Ltd., pp.468-510.

More specific scope or definition can further include, but not limited to, the followings subject to each country's circumstances: e.g.,

- **Unauthorized access with intention to commit further offence**⁴; e.g., computer-related or Internet fraud⁵, and 'theft' of information relating to 'copy right' or 'intellectual property right' misappropriation, forgery etc.
- **Hacking**: e.g., code hackers, crackers, cyberpunks, and phreakers⁶.
- **Destruction of digital information through use of viruses**, logic bombs etc.⁷
- **Harmful sites (e.g., suicide) and contents (e.g., child pornography)** on the Internet:

3. What are the main legal issues in the cyber era ?

One of the critical issues in the cyber era is a matter of **jurisdiction**, which is the authority of a court to hear a case and resolve a dispute within a sovereign territory. Because the legal environment of e-commerce has no geographical boundaries, it establishes immediate long-distance communications with any one who can access the web site. Usually an on line e-merchant has no way of knowing exactly where the information on its site is being accessed. Hence, the jurisdiction issue is of primary importance in cyberspace. For instance, engaging in e-commerce on World Wide Web may expose the company to the risk of being sued in any state or foreign country, where an Internet user can establish a legal claim.

As far as cybercrimes are concerned, the term or scope is still neither clear to many nor have the most countries been equipped with appropriate regulations or laws to prevent cybercrimes. Nevertheless, the main issues of cybercrimes can be largely summarized and classified as below⁸, but not limited to: e.g.,

- **Security**: to deal with e-money (e.g., electronic payments or digital cash) and any misuse or abuse, which led to the needs for encryption, authentication, and digital signature;
- **Hacking or virus**: to deal with damages of digital data;
- **Data protection & privacy**: to protect personal data and privacy;
- **Intellectual property right**: to examine different dimensions especially led by e-commerce in such areas as fixation (e.g., originality and creativity), publication, liability of ISPs, domain names, and encryption;

⁴ [Http://www.newdream.net/bored/messages/15732.html](http://www.newdream.net/bored/messages/15732.html), & [Http://ra.nilenet.com/~mjl/hacks/gtmhh1-2.txt](http://ra.nilenet.com/~mjl/hacks/gtmhh1-2.txt)

⁵ The Internet fraud can be defined as '*any scheme involving Web sites, chat rooms, and e-mail that offers non-existent goods or services to consumers, misrepresents scams a legitimate, or transmits victims' funds, access device, or other items of value to the perpetrator's control*'. Refer to D.Kelsey, 'Feds charge 90 In Web fraud sweep', [Http://www.washtech.com](http://www.washtech.com), May 23, 2001.

⁶ Code Hackers - They know computers inside out and can make the computer do nearly anything they want it to; Crackers - They break into computer systems, Circumventing Operating Systems and their security is their favorite pastime; CyberPunks - They are the masters of cryptography; Phreakers - They combine their in-depth knowledge of the Internet and the mass telecommunication systems.

⁷ Nandan Kamath, 'Crime on the Internet – a challenge', *Law relating to Computers, Internet and E-Commerce: A Guide to Cyberlaws*, 2000, Universal Law Publishing Co. Pvt.Ltd., pp.229-257.

⁸ As for more details, refer to Nishith Desai Associates, 'Legal & policy framework for e-commerce in India', edited by Nandan Kamath, *op.cit.*, 2000

Apart from such relatively well pointed issues as security, hacking or virus, privacy and IPR, indeed, there are many other issues with which individuals and businesses must be familiar when using the Internet and the World Wide Web. The potential legal issues or even questions raised from the cyber-activities include as follows: e.g.,

- Do users approve of the insertion of anything in to their computers without their knowledge and consent?
- Can sale made on the Internet be taxed⁹?
- What constitutes defamation on the Internet?
- Is web content protected by copyright law?
- How can laws relating to the Internet be enforced ?
- How can consumers be protected ?

Concerning gender-sensitive issues, *harmful sites* and/or *contents* can be closely looked at whether they contain any offensive or violating materials against women, particularly girl-children.

In consideration of all these issues under the scope of cybercrimes subject to each country's jurisdiction and their impacts on global socio-economy beyond the jurisdictions, we may need to be more aware of them and take appropriate legislative measures to govern the cyber-world before it is too late.

4. What kind of legislation may be required against Cybercrimes ?

In view of the rapid growth in the converged ICT sectors, countries around the globe have started to equip their legislation with either resorting to amend their existing legislation or to enact new legislation to suit the requirements from cyber-activities or cyber-crimes, as a few examples are illustrated in Table 1.

<Table 1: Trends of Legislation on Cyber-crimes & Cyber-activities>

Countries	Cyberlaws	Other-related Laws
UK	Computer Misuse Act (1990)	
India	Information Technology Act (2000)	IPR Law
Hong Kong Singapore Thailand	Electronic Transaction Act	Copyright Law Trade Marks Law
Philippine	E-commerce Act	
Germany Italy etc.	Digital Signature Laws	
R.O.Korea	Privacy Law	Patent Law

⁹ Chetan Nagendra, 'An introduction to the Indian tax structure and the challenges posed by Internet commerce', edited by Nandan Kamath, *op.cit.*, 2000, pp.351-369.

5. What is the scope of Cyberlaw: A case of the Information Technology Act, India ?

India has enacted the first cyberlaw to foster the advantages of new technologies - i.e., ICTs - as well as to tackle some of the emerging issues on cyber-activities or crimes. For instance, the Act proposes facilitation of:

- Electronic commerce transactions;
- Maintenance of electronic records; and
- Electronic government transactions.

The Act also provides for a legal framework for *validation of information in electronic form* and deals with the major issues as follows, but not limited to: e.g.,

- **Securing electronic transactions:** These enable parties to enter into electronic contracts.
- **Attribution of electronic messages:** i.e., Once the message leaves the information system of the originator of the message, it is attributed to him.
- **Electronic signatures and electronic records given legal status.** In furtherance of this, and to maintain security of information, the Act establishes a Digital Signature Infrastructure making specific use of the Asymmetric Crypto System Technology with new authorities such as the Controller of Certifying Authorities being set up.
- **‘Contraventions’** regarding electronic records viz. hacking theft of electronic records, manipulation of records, spreading viruses, etc. have been defined. Involved in the inquiry and determination of the result of the proceeding is an adjudicating officer, appointed by the Government and possessing wide-ranging powers.
- Information Technology Offences viz. tampering with computer source documents - i.e., **obscenity**. A limited number of offences have been created under the Act. These will be tried as any other criminal offences, which are under the Criminal Procedure Code but with unique provisions for investigation, search, etc., provided in the Act.
- **Right of government bodies** to decrypt information has been specifically given herein.
- **Privacy and confidentiality of information** submitted to statutory authorities. Dissemination to third parties of such information collected in pursuance of powers under the Act is made a criminal offence.
- **Facilitates e-commerce** as well as **electronic filing and maintenance of records** as against the government.
- Setting up of **new authorities/regulatory infrastructure:** e.g., cyber regulatory authorities such as the controller of Certifying Authorities and the Cyber Regulations Appellate Tribunal (CRAT) have been established. The Act also seeks to set up a Cyber Regulations Advisory Committee (CRAC).
- **Liability of Internet Services Providers for content** on the Internet is limited in so far as the provider exercises all due diligence. This is relevant in connection with copyright violations, pornography, etc., residing on various web pages or moving through the systems of the ISP.

6. Any gender-sensitive Cyberlaw ?

As cyber-activities are relatively young, so are there less awareness and enforcement of gender-sensitive legislation in most countries. However, the major issue or concern about gender-sensitive cyberlaws is relating to *harmful sites* and/or *contents* in addition to various legal issues described earlier on.

Most countries except India, which has reflected such issues as *obscenity* in her new IT Act, have not yet been aware of the needs for gender-sensitive legislation against the harmful sites and/or contents in ICT. If so, they rather tend to accommodate such gender-related cybercrimes through the nets into their existing laws rather than to enact new laws, as some examples are illustrated in Table.2.

<Table 2: Examples of Gender-sensitive Laws>

Countries	Gender-sensitive Laws
India	Penal Law & IT Act
Hong Kong	Obscenity Law
USA	Communication Decency Act
UK	Obscene Publication Act
EU	Self-regulation

7. Legislative ways forward against Cybercrimes ?

Ways of tackling cybercrimes through legislation may vary from one country to another, especially when cybercrimes occur within a specific national jurisdiction with different definition and socio-political environment.

For example, Internet or its usage may be censored from the grass-root, as some governments (e.g., Singapore, China, and Vietnam¹⁰) have sought to control their citizen's use of the Internet, either by forcing users to register with governmental monitoring organizations or by directly controlling Internet traffic coming into their countries through government-controlled ISPs at least in the early days. Whilst, the FCC¹¹ (USA Administration) together with private industries¹² is in favor of 'unregulation' of Internet at markets or 'self-regulation' by industries themselves especially in the areas of privacy or personal data protection. In case of Korea, NGOs led by civil associations began to work together so as to prevent harmful sites such as 'suicide', which caused lots of suicidal accidents. Furthermore, the US-based Internet Fraud Complaint Center (IFCC) is playing a mediating role to receive complaints from 89 different countries and refer to the relevant law enforcement agencies.¹³

In the world of a global information infrastructure – beyond national jurisdictions, an escalating national *de jure* regulation meets a similarly pervasive *de facto* futility of enforcement. National legislatures might continue to enact regulations especially over criminal matters, but their regulatory endeavors are unlikely to be effectively enforceable, as they desire due to the global nature of ICTs. In principle, a global phenomenon in the ICT sectors - especially the Internet - should propel nations to achieve legal and regulatory co-operation and partnership at international levels, since cyberspace is no respecter of national boundaries.

¹⁰ Refer to [Http://www.unikonstanz.de/~dierk/censorship/countries.html](http://www.unikonstanz.de/~dierk/censorship/countries.html).

¹¹ William E. Kennard (ex-FCC Chairman), "We can have openness and competition by following the FCC's tradition of "unregulation" of the Internet", A speech before the Federal Communications Bar, Northern California Chapter, San Francisco, CA, July 20, 1999, [Http://www.fcc.gov](http://www.fcc.gov).

¹² [Http://www.cisco.com/public/privacy.html](http://www.cisco.com/public/privacy.html)

¹³ D.Kelsey, *op.cit.*

With this view, international approaches are considered to be one way of overcoming or solving the current cybercrimes occurred particularly beyond national jurisdictions. An international legal instrument (*jus cogens*), which by definition embodies this global consensus and positively binds all nations, could provide a useful tool in drafting a possible solution (*jus cogens*) limiting regulation to specific and defined areas of cybercrimes together with creative international enforcement structures, which might facilitate the creation of both sensible and feasible regulations in such forms as global conventions, multilateral treaties, international law, global standards (e.g., ITU, ISO etc.) for certainty and security, model uniform laws (e.g., UNITRAL etc.), and model contracts/standard terms.

In this context, recognizing such needs for global cooperation and harmonization to prevent or solve cybercrimes in the ICTs, the Member States in Asia and Pacific region of the ITU recently recommended the Union to “*develop model laws or guidelines on legislative issues in ICT, especially taking into account socio-economic concerns such as cybercrime*” and “*support initiatives aimed at establishing international regulatory principle(s) with regard to cybercrime.*”¹⁴

To summarize, as cyberlaw is the state of infancy and evolutionary stage, various legal issues including gender-sensitivity need to be settled in the due course of time. While all the nations need to review their traditional legislation and make appropriate legislative measures to suit the new ways of human activities, international organizations like the UN also need to play an important role to create appropriate international regulations or treaties for the effective governance of cyberspace.

¹⁴ Document 64, 'Policy, legal & regulatory priorities, The Asia & Pacific Region', *Regional Preparatory Meeting for the World Telecommunication Development Conference, Asia and Pacific Region*, Bali, April 24-27 2001.