POLICY CONSIDERATIONS IN INDIA AGAINST CYBER CRIME

Jitender Kumar Malik* and Sanjaya Choudhary
Department of Law Bhagwant University (Raj.) India

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0912.2936

INTRODUCTION

Michael A Sinks, argues that, 1 in land, sea, and air battles, military combatants can see the enemy coming, whether it’s the whites of their eyes or a blip on a screen. International boundaries easily define when an aggressor threatens the sovereignty of a nation, giving the victim nation the right of jurisdiction, and there are specific international laws that address military operations in space. In addition, the international community has defined when an adversary’s use of force threatens a nation's territorial integrity and political independence. However, the global nature of cyberspace and the speed of which victims can experience cyber attacks force nations to deal with the legal challenges associated with over-the-horizon military operations.

Cyber crime is the deadliest epidemic confronting our planet in this millennium. A cyber criminal can destroy websites and portals by hacking and planting viruses, carry out online frauds by transferring funds from one corner of the globe to another,
gain access to highly confidential and sensitive information
cause harassment by e-mail threats or obscene material, play
tax frauds, indulge in cyber pornography involving children
and commit innumerable other crimes on the internet. It is said
that none is secure in the cyber world. People with intelligence
have been grossly misusing this aspect of internet to perpetuate
illegal acts in cyber space. The field of cyber crime is just
emerging and new forms of criminal activities in cyber space
are coming to the forefront with the passing of each new day.
Cyber crimes may range from 'the merely annoying' to 'the
catastrophic.' Gurmanpreet Kaur, Anand Pawar and
Simranpreet Kaur conclude that the only possible step to make
people aware of their rights and duties is to make the laws more
stringent to keep a check on crimes.¹

Cyber crime, today, have increasingly emerged as major
challenges for nations across the world. The fact that Internet
has made geographical history has further facilitated cyber
criminals to perpetuate their criminal designs and activities
across networks. The transnational nature of cybercrimes has
further complicated the challenges for national governments to
regulate cyber criminal activities. As such, national
governments are adopting their national legislations for
regulating cyber crimes. India has come up with its own
regulatory regime with aimed at cyber fraud and cybercrimes.
Pavan Duggal’s book Cyber Frauds, Cybercrimes & Law in
India² looks at the way of how Indian cyber law addresses
cyber fraud and the various cybercrimes and quantum of
punishments for it. The book and further looks at what are the
challenges being faced by the Indian legal regime while
regulating cybercrimes; and the deficiencies of the Indian
approach in dealing with cybercrimes.

In his work³ of felt need round the globe- Cyber Crime in
India-A Comparative Study, the experienced author has
discussed the intricate problems that are being faced by the
international community every moment and also their probable
solutions. With advancement of technology the cyber criminals very
often trespass, destroy or alter computer, computer system, computer
programme, software, network and related devices. While dealing
with this emerging subject the author has taken adequate care to
corporate the issues like classification, nature and elements of cyber
crime, activities of the cyber hackers, cyber frauds, cyber
pornography, online child pornography, cyber terrorism and so on.

Police Investigation Powers, Tactics and Technique⁴ is a benchmark
and best-practice model and regarded as the ‘Bible’ for professional
investigation in India. Anchoring himself firmly on the ever-contested
space of Indian law and legal processes, and drawing substantive
support from his rich and varied experience as a law enforcement
officer in the police department, the author, has sought to fulfill the
legitimate requirements of police officers, advocates, judicial officers,
social activists, NGOs, gender activists and the general public. The
author's utopian ideal that no innocent person should be punished and
no offender should go unpunished is the dominant message of the
book. The citation of more than 800 landmark judgments of various
High Courts and the Supreme Court for the period 1965-2016 in the
appropriate chapters is another outstanding feature of the book.

Cyber Crimes against Women in India⁵ reveals loopholes in the
present laws and policies of the Indian legal system and what can be
done to ensure safety in cyberspace. The book is a significant
contribution to socio-legal research on online crimes targeting
teenage girls and women. It shows how they become soft
targets of trolling, online grooming, privacy infringement,
bullying, pornography, sexual defamation, morphing and so on.

The authors address various raging debates in the country such
as how women can be protected from cybercrimes; what steps
can be taken as prevention and as recourse to legal aid and how
useful and accessible cyber laws are.

Banks are offering many services of which, the electronic mode
is becoming popular amongst Banks and their customers.
Presently, these are in the form of ATMs, credit & debit cards,
online transactions, net banking, mobile banking, e-commerce,
new payment systems etc. As more and more services of banks
are offered in electronic mode, they must be aware of the risks
due to possible misuses of new technology based services and
various online channels. It has become important that the
bankers, particularly who are dealing with I.T. and online
channels, would be well versed with the various cyber crimes
and frauds which may occur in offering these services. To
safeguard the interest of the banks and their clients, a banker
who is dealing in such services should have thorough
knowledge and understanding about cyber crimes and how to
mitigate a fraud and prevent eventualities in future. The book;
Cyber Crimes and Fraud Management provides an overview of
various types of cyber crimes and how to alleviate such crimes.⁶

Computer Internet and New Technology Laws⁷ is a comprehensive work that aptly highlights new laws, policies,
cases, concepts, events and studies that have evolved cyber
laws in the national and international spheres. It specially
focuses on the development of laws in India including new bills
and guidelines that were passed such as Electronic Delivery of
Service Bill, 2013, the cabinet approval of the New Consumer
Protection Bill 2015 and the new guidelines for the
introduction of e-authentication technique using Aadhar-eKYC
services. It also discusses land mark cases, including Shreya
Singhal v. UOI, which struck down Section 66A of the IT Act,
2000 as unconstitutional and Anwar v. P.K Basheer which
clarified the law on appreciation of electronic evidence in
India. The book critically examines the emerging crimes such as
trolling, sexting and revenge porn and new developments
such as Net Neutrality that have impacted the cyber world. The
work cover recent amendments and new Rules related to
Protection of Children from Sexual Offences Act 2012,
National Cyber Security Policy 2013, IPR policy, Guidelines
for Foreign Direct Investment in India, Directives on Consumer
Rights, Regulation on Data Protection Rules within European
Union and more.

John Dickie outlines and analyses the legislative activity of the
European Union in an area which is currently experiencing
exponential growth in terms of both commercial activity and
legal significance.⁸ He has taken great pain in incorporating the
current, pending and proposed Internet-related law on
contracts, copyright, data protection, commercial
communications, financial services, electronic cash and
electronic signatures; and submits that the European Union is
in the process of displacing Member State autonomy in the
regulation of the Internet. Within that frame, it is argued that
there is a lack of focus on the individual in the electronic
marketplace and a lack of co-ordination between relevant legislative instruments.

The only casebook dealing with e-commerce, *Electronic Commerce*, utilises problems to expound a transactional approach to electronic commerce. Ronald J. Mann attempts a hypothetical representation of a technology company. The work provides a detailed discussion on click-through contracts, cyber-squatting, web site development, software licensing and electronic payments.

At a time when there are still a number of voices calling for the Internet to remain a law-free zone, a whole bundle of conflicts have already emerged, many of which have found their way to lawyers and the courts in a substantial number of different jurisdictions. It surely now cannot be doubted that the Internet, like any other place in the world where people come together and follow their own interests, needs rules to be developed for the handling of such conflicts. Lawyers have already reacted and have created a new area of law—commonly called "law of the internet" or "cyber law." This area, however, is still far from being strictly defined. It touches on many existing areas of law, but at the same time it deals with a wholly new medium—cyberspace—which itself is subject to constant change and development. Under these circumstances, it is not surprising that in a number of cases the predictions as to how this law will look at some selected moment in the future are vague and uncertain.

In order to provide an overview of the most important legal issues of E-Commerce Gerald and Borne* describe the regulatory framework in nine European countries (Belgium, France, Germany, Great Britain, Italy, Norway, Spain, Switzerland and Nether lands) and the United States of America. The country-specific contributions present an overview of the main questions and trends in E-Commerce Law, in particular with regard to the adoption of several EU Directives.

An Indian author, in his work discusses various legal issues in electronic commerce and states how legislation in other countries has sought to solve them. It also discusses the beginning made by Information Technology Act, 2000 in India. There are many important issues which are critical for the success of e-commerce that have not been covered or properly addressed by IT Act. Dr. Sumantjeet reveals that the present IT Act is weak on various fronts and in the absence of sound legal framework e-commerce cannot create a success story in India. Indian Government must appreciate that for safe and secure business environment on cyberspace, a sound legal framework is needed. His paper suggests that there is strong need to introduce separate laws for e-commerce in India. After having critically examined the Indian IT Act 2000 and IT (Amendment) Act 2008 in the light of e-commerce perspective to identify the present status of e-commerce laws in India, the author identifies various loopholes in the existing e-commerce laws in India; and suggests measures to protect the interests of Indian software industries, BPO sector and other stakeholders.

Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce captures the essence of the Information Technology Act, 2000; discusses and analyses in great detail different aspects related to the subject and the challenges posed by information technology. Issues related to cyber-crime, virtual currency (bit-coin), Internet blocking, sexting, child pornography, surveillance, cyber terrorism, encryption, digital India, social media, cyber security have been discussed in the legal context. Further, considering the nature of the subject and the international perspective, it provides a comparative analysis of corresponding provisions in other jurisdictions. Hundreds of judgments, including that of Shreya Singhal, Aadhaar, Bazee, etc. have been interwoven seamlessly to underline the way judges have been weaving technology with judicial wisdom and coming out with judicial interpretation of various facets of technology.

**CONCLUSION**

The power of the Web to reach the world carries with it a variety of legal issues, often related to intellectual property concerns, privacy, decency, etc. Authorities seeking to apply their laws in traditional ways or to expand legal control over international links face many challenges due to the global nature of the internet. A comprehensive policy and legal framework to regulate cyber crimes is the need of the hour. In this backdrop, the present study assumes significance.

**Bibliography**

12. Debarati Halder & Jaishankar, Cyber Crimes against Women in India (Sage Publications, 2016)

**How to cite this article:**

*******