Inspira-Journal of Commerce, Economics & Computer Science (JCECS)
p-ISSN : 2395-7069 (Impact Factor : 2.0546) Volume 03, No. 02, April - June, 2017, pp. 160-164

CYBER LEGISLATION AND FRAMEWORK: A REVIEW

Dr. Rajeev Srivastava*
Rajesh Koolwal**

ABSTRACT

Cyber Legislation examines the role of regional as well as national law and frameworks in the aversion and combating of cybercrime. It finds that legislation is required in all areas, including criminalization, procedural powers, jurisdiction, and international cooperation. While the last decade has seen significant and major developments in the annunciation of multilateral instruments aimed at countering cybercrime, that highlights a growing legal fragmentation at national and regional level.

***KEYWORDS**: Cyber Legislation, Framework, Combating of Cybercrime, Multilateral Instruments.*

Introduction

Legal measures play a vital role in the prevention and combating of cybercrime. Law is dynamic apparatus that empowers the state to react to new societal and security challenges, such as, fitting harmony between privacy and crime control, or the degree of obligation of organizations that provide services. The innovative improvements related with cybercrime imply that – while conventional laws can be applied to some degree – legislation should likewise deal with new ideas and items, not generally addressed by conventional laws. In many states, laws on innovative improvements go back to the nineteenth century. These laws were, and to a great extent, still are, focused on *physical* objects – around which the daily life of industrial society revolved. For this reason, many traditional general laws do not take into account the particularities of information and information technology that are associated with cybercrime and crimes generating electronic evidence. These acts are largely characterized by new *intangible* objects, such as data or information.

Physical items can usually be ascribed only to specific proprietors, for instance, to the legitimate idea of 'burglary', connected in the customary laws of numerous nations. A 'burglary' of PC information, for example – even given the expansion of the idea of items to incorporate information or data – may not fall within the scope of the constituent components of conventional burglary. The information would in any case stay in the ownership of the first conveyor, therefore relying on national law approaches, perhaps not meeting required legitimate components, for example, 'expropriation' or 'taking' of the object. Additionally, legitimate references to a public or private 'place' in harassment or stalking laws may, or may not again, depending upon national approaches, stretch out to online 'spots.' Such examples illustrate a potential need – in some areas – for the adaptation of legal doctrines to new information technologies.

---

* Research Guide, Mahatama Jyoti Rao Phoole University, Jaipur, Rajasthan & Principal, LBS P.G. College, Jaipur, Rajasthan.

** Research Scholar, Mahatama Jyoti Rao Phoole University, Jaipur, Rajasthan & Lecturer, Department of Computer Science, LBS P.G. College, Jaipur, Rajasthan.