Chapter 15
Dispute Settlement for Cyber Crimes in India: An Analysis

Rashmi Aggarwal
IMT Ghaziabad, India

ABSTRACT

Cyber law is law of the Internet; hence, any crime on the Internet is basically cyber crime. It is committed on cyber space, but all the pre mediation is an act of individual/s, who are the perpetrators of crime with malicious intentions and commission of these acts. Cyber crimes were initially perceived as a subset of Information Technology (IT) laws, which governed the digital dissemination of both digitalized information and software. Digital information includes information security and electronic commerce. However, as the world became subservient to digitalization, cyber/Internet laws became more pronounced in their origin and are now a special branch of Internet laws. These laws include study of Internet access and usage, privacy rights, freedom of expression, and extra territorial jurisdiction issues. This chapter analyzes the cyber laws in India and raises the issues of criticality of provisions relating to dispute resolution in India.

INTRODUCTION

The first cyber crime took place in the year 1820 in France. In the modern era, the first few instances of cyber crime date back to 1978 when first spam email was sent over the ARPANET (Advances Research Projects Agency Network). The 1982, first virus was installed on an Apple computer when Rich Skrenta, a high school student, developed the ELK clone. The cyber crimes are committed against persons, individual property, or government. These are committed in three ways: The computer as a target, attacking the computers of others for example hacking, virus/worm attacks, DOS attack extra. The computer as a weapon where a computer is used to commit “traditional crime,” the real world crimes. For example- fraud, illegal gambling, cyber terrorism, IPR violations,
credit card frauds, pornography extra. And lastly, using computer as an accessory, i.e. a “fancy filing cabinet” to store illegal or stolen information.

The Information Technology, inventions, and discoveries widen the scientific horizons but pose new challenges for the legal world. Therefore, solutions for the disputes arising out of these challenges, whether statutory or otherwise, are referred as the “Cyber Laws.” European Union, USA, United Nations Commission on International Trade Law (UNCITRAL) have already framed important laws to regulate cyberspace. In India, Information Technology Act (ITA) is also based on UNCITRAL model, all cyber laws are contained in Information Technology Act, 2000.

Cyber Crime in India

Statistical data on cyber crime in India is recorded by Ministry of Home Affairs under the National Crime Record Bureau. And according to them, 1,791 cases were registered under IT Act during the year 2011 as compared to 966 cases during the previous year (2010) thereby reporting an increase of 85.4% in 2011 over 2010. 19.5% cases (349 out of 1,791 cases) were reported from Andhra Pradesh followed by Maharashtra (306), Kerala (227), Karnataka (151), and Rajasthan (122). Out of these 46.1% (826 cases) of the total 1,791 cases registered under IT Act 2000 were related to Loss/damage to computer resource/utility reported under hacking with computer systems. 487 persons were arrested for committing such offences during the year 2011. There were 496 cases of Obscene publications/transmission in electronic form during the year 2011 wherein 443 persons were arrested. Out of total (983) Hacking cases, the cases relating to Loss/Damage of computer resource/utility under Sec 66(1) of the IT Act were 84.0% (826 cases) whereas the cases related to Hacking under Section 66(2) of IT Act were 15.9% (157 cases). Andhra Pradesh (267) followed by Karnataka (87), Rajasthan (69), and Maharashtra (68) registered maximum cases under Sec 66(1) of the IT Act out of total 826 such cases at the National level.

Out of total 157 cases relating to Hacking under Sec. 66(2), most of the cases (23 cases) were reported from Karnataka followed by Kerala (22) and Andhra Pradesh (20 cases). 20.4% of the 1184 persons arrested in cases relating to IT Act, 2000 were from Andhra Pradesh (242) followed by Maharashtra (226). The age-wise profile of persons arrested in Cyber Crime cases under IT Act, 2000 showed that 58.6% of the offenders were in the age group 18 – 30 years (695 out of 1184) and 31.7% of the offenders were in the age group 30 - 45 years (376 out of 1184). Madhya Pradesh (10), Maharashtra (4), Kerala (3), and Delhi (2) reported offenders whose age was below 18 years. Further, 41.1% (487 out of 1184) of the offenders arrested were under ‘Loss/damage to computer resource/utility under hacking with computer systems’ of which 53.3% (260 out of 487 were in the age-group 18 –30 years. 63.8% (283 out of 443 persons) of the total persons arrested for ‘Obscene Publication/Transmission in Electronic Form’ were in the age-group of 18 - 30 years. Hence the statistical data are indicating the dire trends of cyber crime in the country. Cyber Crimes increased by 22.7% in 2007 as compared to previous year. Cyber Forgery 64.0% (217 out of total 339) and Cyber Fraud 21.5% (73 out of 339) were the main cases under IPC category for Cyber Crimes. 63.05% of the offenders under IT Act were in the age group 18-30 years (97 out of 154) and 55.2% of the offenders under IPC Sections were in the age group 30-45 years (237 out of 429). According to analysts at the Indian Institute of Science, Tax evasion, cheating on the Internet, identity theft, child pornography and other cyber crimes cause a loss of $50 billion annually.

Defining Cyberspace

Cyberspace is the electronic medium of computer networks, in which online communication takes place. It is governed by a system of law and
Related Content


Self-Assessment of Principals Based on Leadership in Complexity

Participation of Women in Logistics Through Innovation