Chapter 29
Legal Regulation of Cybercafés:
The Indian Experience

S.R. Subramanian
Hidayatullah National Law University, India

ABSTRACT

Cybercafés constitute the most important model of public access to Internet, especially in developing countries. They compensate those who temporarily or permanently lack access to the Internet. However, the deeper and the wider penetration of the Internet also increased the opportunities for misuse of technologies. Due to a number of reasons, cybercafés have the huge potential for facilitating a number of crimes, impacting privacy, property, contracts, and even national security. This chapter argues that it is an imperative to regulate these entities as a preventive measure to avert cyber-crimes and terrorism. Drawing the example from India and adopting the legal approach, this chapter captures the legal developments relating to the regulation of cybercafés in India. It is expected to shed valuable insights for other countries contemplating the institutionalization or proposing changes in their regulatory framework. The chapter concludes that a well-orchestrated policy on cybercafés, taking into account the environmental variables of the particular country, is a pre-requisite for the ICT policy of any country.

INTRODUCTION

Information and communication technologies (ICTs) being transformative and revolutionary in nature, promoting access to technologies is critical to all areas of development. Moreover, today even there is a talk of Internet access as a human right, which demonstrates the inevitability and dependability of network access (Hick, Halpin & Hoskins, (2000). Studies of Internet users reveal that public internet facilities are the important component of access to information and communication technologies next to home use and access at workplaces (Haseloff, (2005). Though there is a perceptible change in this profile in the recent times, still cybercafés constitute the

DOI: 10.4018/978-1-61520-847-0.ch029

most important model of public access to Internet, especially in developing countries. They compensate those who temporarily or permanently lack access to the Internet.

However, the deeper and the wider penetration of the Internet also increased the opportunities for misuse of technologies. The increase in cybercafé-facilitated crimes are due to a number of factors including the proliferation of Internet access points, lack of proper and adequate legal regulation and the anonymity of the cybercafé operations itself. Accurate statistics about the diffusion and the penetration of the cybercafés are unavailable mainly due to the differences in the definition of cybercafé (Arnold, 2008). The rough estimates are that there are around 200,000 cafes in the world (Arnold, 2008), with the figures for India.

India is recognized as the global hub of information technology and its allied services. It is attributed to have 81 million users of Internet (Economic Times, 2008) and among them a 37% prefer the access at the Internet access point (Ramachandran, 2009). The unofficial figures of total number of cybercafés in India are around 50,000 (Arnold, 2008). As the cybercafés have the huge potential for facilitating a number of crimes, impacting privacy, property, contracts, and even national security, it would be prudent on the part of government to monitor and regulate their operations.

Drawing the example from India, this paper analyses the problems of regulating the cybercafés in a federal constitutional set-up. In particular, it examines the issues of 'which entities are cybercafés', the scope of their regulation, the administrative problems and the human rights concerns in regulating them. As there is no legal provision in the (Central) Information Technology Act, 2000, in respect of their regulation, it has taken for analysis some of the pioneering initiatives by the Indian states.

THE NEED FOR REGULATING THE CYBERCAFÉS

Though a number of traditional and computer crimes can be committed in the cybercafes, the high number of visitors to the cybercafé and the relative anonymous feature of the cybercafé chambers afford the users an increasing level of opportunities to commit a range of crimes. Some of the common crimes committed in the premises of or facilitated by the cyber-café, as reported by the Indian media are:

a. Sending anonymous emails to cause annoyance, insult and injury etc, (e.g. misleading information causing unnecessary patrolling at airports etc.,) (New Delhi News, 2007),
b. Stealing the personal identification details of another user (Akhtar, 2008),
c. Use of Internet for carrying out any terrorist purposes, such as propaganda and recruitment etc by banned groups (Express News Service, 2009),
d. Taking advantage of the extra privacy for accessing, viewing pornographic sites etc., (Chada, 2009),
e. Facilitating intellectual property violations (Kumar, 2009) and
f. Facilitating the commission of any computer-related crimes (Kumar, 2009).

CYBERCAFÉ REGULATION AND THE INDIAN INFORMATION TECHNOLOGY ACT, 2000

The original Information Technology Act, 2000 virtually had no specific provision to deal with the cybercafés. Nor the term 'cybercafé' was defined in the parent Act or even in the Rules. However, the general provisions concerning the network service provider's liability was also extended to cyber-cafes. Section 79 of the Act seeks to

Related Content

Does Innovation Flourish With the Implementation of Certified Management Systems?: A Study in the European Context
Vasileios Mavroeidis, Petros E. Maravelakisand Katarzyna Tarnawska (2020). *Shaping the Future Through Standardization (pp. 149-167).*
www.irma-international.org/chapter/does-innovation-flourish-with-the-implementation-of-certified-management-systems/247400

Energy Efficiency Standards: The Struggle for Legitimacy
Abdel Fattah Alshadafan (2020). *International Journal of Standardization Research (pp. 1-17).*
www.irma-international.org/article/energy-efficiency-standards/270252

Password Sharing and How to Reduce It
Ana Ferreira, Ricardo Correia, David Chadwick, Henrique M.D. Santos, Rui Gomes, Diogo Reisand Luis Antunes (2013). *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 22-42).*
www.irma-international.org/chapter/password-sharing-reduce/75023

Structural Effects of Platform Certification on a Complementary Product Market: The Case of Mobile Applications
Ankur Tarnachaand Carleen Maitland (2008). *International Journal of IT Standards and Standardization Research (pp. 48-65).*
www.irma-international.org/article/structural-effects-platform-certification-complementary/2594

Modularity of the Software Industry: A Model for the Use of Standards and Alternative Coordination Mechanisms
Heiko Hahnand Klaus Turowski (2005). *International Journal of IT Standards and Standardization Research (pp. 29-41).*
www.irma-international.org/article/modularity-software-industry/2566