

Chapter 37

Regulation of Cybercafés in Nigeria

Mercy Eyitemi
Delta State University, Nigeria

ABSTRACT

The purpose of this chapter is to discuss regulation of cybercafés in Nigeria. It describes cyber crime in relation to cybercafé, the incidents of cybercrime as well as crime associated with cyber usage. The chapter reveals why cybercafés are used as havens for cybercrimes in Nigeria and looks at efforts made by Nigerian government to regulate cybercafé as well as challenges of regulating cybercafés in the country.

INTRODUCTION

Cybercafé which is also known as Internet café is a place where people can get connected to/access the internet. Modern cybercafés also have wireless connection in their local area (LAN), where people can bring their own lap tops and get connected to the internet by paying a small fee. (Google, 2007).

In Nigeria, cybercafés have become an integral part of the business, and social environment. They appeared as a result of the introduction of the internet which gave rise to the widespread use of instant electronic communication among people, irrespective of their location. Cybercafés have

developed to a booming business as the internet has been found to be useful for business transaction, education, entertainment and everyday communication. As a result of this, cybercafés are springing up in major cities in Nigeria in order to meet the needs of members of the society. Also cybercafés have become a hit in Nigeria because of limited telecommunication infrastructure in the country. (Tiemo & Iyoha, 2008).

Cybercafés are set up in order for entrepreneurs to make money and to enable their clients access the Net. Ayatokun (2006) pointed out that convenience associated with information technology (IT) and the internet is now being exploited to serve criminal purposes. Also, Emiri (2008) observed that information technology is a double edged sword, which can be used for destructive purposes

DOI: 10.4018/978-1-61520-847-0.ch037

as well as constructive work. Thus cybercafés can be used by cyber criminals to launch attacks on individuals and organisations. Criminals can explore the anonymity provided by cybercafés to commit cyber defamation, terrorism, hacking, etc. (Adomi, 2008).

In order to stem the incidents of crimes committed in cybercafés, the Nigerian Government has taken some steps to regulate the operations of cybercafés in the country. One of such was the recent enactment of the “Advance Fee Fraud and other Related Offences Act, 2006”. These measures have been taken in order to help correct negative international image which cyber crimes have brought to the country. There are some challenges facing these laudable Government efforts at present.

The purpose of this chapter is to explore the cybercafé regulatory efforts of Nigerian Government. It dwells on incidents of cybercrime; crimes associated with cybercafé usage, why cybercafés are used as havens for cybercrime in Nigeria; government efforts to regulate cybercrime in cybercafés; challenges of regulating cybercafés and future trends of control of cybercafés in Nigeria.

BACKGROUND

A cybercafé is a general place where people can access the internet for a fee. A cybercafé is a place where people can get connected to the internet by using publicly accessible computer. It could have 10 or more computers for clients, devices (printers, scanners, routes etc) and a server used for a remote administration and which share common resources. (Ajewole, 2008)

Cybercafé could be described as a virtual market where all kinds of business transactions take place. Adomi, Okiy and Ruteyan, (2003) define cybercafés as places where entrepreneurs provide internet public access services for a fee. They have been variously described as places where people of diverse culture and characters

meet and engages in internet surfing and e- communication. There is proliferation of cybercafés especially in developing countries because of two strong drives: because people want to make money by opening/operating cybercafés and many users want to surf the internet which offer easy access to news reports, chat rooms, pornography, gambling, exchange of letters and so forth (Igun, 2008). Cybercafé play an important role in accessing information and communication technology (ICT) particularly in region of economic deprivation or low infrastructural development (Adomi, Okiy & Ruteyan, 2003; Mutala, 2003; Adomi, 2008).

Regulation according to the Hornby, (2000) is an official rule made by a government or some other authority. The rules, laws and acts enacted by government in order to regulate the behaviour and activities of individuals and organizations are regulations.

Cyber crime has to do with unlawful conduct carried out with the use of computers, electronic and ancillary devices. It involves disruption of network traffic: denial of service attacks/e-mail bombing, creation/distribution of viruses, identity theft, cyber stalking, cyber squatting, pornography, extortion, fraud and impersonation. (Adomi & Igun, 2007).

Activities of cyber crime include abuse of credit cards, pornography, cyberspying, cyber stalking, spamming, hate crime, solicitation, cyberpiracy, money laundering and bribery. In spite of the fact that cyber crime is a criminal activity, a lot of jurisdictions have been faced with challenges in resolving litigation arising; in this context, of the activities surrounding cyber crime. Such challenges which involves identifying the origin of the crime/location of the offenders, requires active laws to be applied in trying the offender among others. Cyber crimes are, to a great extent, committed in cybercafés and this occurs both in the developed and developing countries. Since cybercafé is a commercial premises or operation which allows people to use computers with internet access for a fee, it is important for operators

7 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/regulation-cybercafés-nigeria/45411

Related Content

Analysis of ISO 9001 Paradox of Knowledge Codification Using the Activity System Model: Tensions in Practices and Expansive Learning

Hiam Serhanand Doudja Saïdi Kabèche (2017). *International Journal of Standardization Research* (pp. 37-56).

www.irma-international.org/article/analysis-of-iso-9001-paradox-of-knowledge-codification-using-the-activity-system-model/202987

Global Perspectives on the Information Society

William J. McIver Jr. (2004). *Social, Ethical and Policy Implications of Information Technology* (pp. 1-28).

www.irma-international.org/chapter/global-perspectives-information-society/29303

Analysis and Validation of Learning Technology Models, Standards and Specifications: The Reference Model Analysis Grid (RMAG)

Jan M. Pawlowski and Denis Kozlov (2010). *International Journal of IT Standards and Standardization Research* (pp. 1-19).

www.irma-international.org/article/analysis-validation-learning-technology-models/46109

Standardization and Other Coordination Mechanisms in Open Source Software

Tineke M. Egyedi and Ruben V.W.D. Joode (2006). *Advanced Topics in Information Technology Standards and Standardization Research, Volume 1* (pp. 71-90).

www.irma-international.org/chapter/standardization-other-coordination-mechanisms-open/4657

Information Security Policies

J.R Ikoja-Odongo (2011). *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements* (pp. 434-448).

www.irma-international.org/chapter/information-security-policies/45399