IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 21, Issue 1, Ver. I (Jan. 2016) PP 18-24
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Digital Age 2.0 and its challenges on media ethics

Juhi P. Pathak
Asst. Professor, Amity School of Communication, Amity University, Noida, UP.
Former Junior Research Fellow (UGC) & Ph.d Research Scholar, Department of Communication and Journalism, Gauhati University, Assam, India

Abstract: *We are currently living in the digital age, more commonly known as the Information Technology (IT) Age; which can be described as an era where every aspect of human life or activities are mainly information based. This is due to the development and use of technology. We live in a world that has become more open - in the sense of communication (global village) and internationalization (trans-border flow of data).*

The revolution in Information technology is having its implications on our access to information. The digital space provides us with a vast expanse of data and information on a domain that is easily accessible to all. And as such the ethical aspect with regards to the data get threatened.

This paradigm shift in this digital age brings new ethical problems which are mainly related to issues of media laws; such as the right of access to information, the right of privacy which is threatened by the emphasis on the free flow of information, and the protection of the economic interest of the owners of intellectual property.

In this paper the ethical questions related to technology and its implications on media laws and ethics will be discussed. Specific attention will be given to the challenges these ethical problems pose to the information on the digital space.

Keywords: *Digital age, Internet, Violation, Media Ethics, Privacy*

Objectives

1. To make an analysis if the paradigm shift in the digital age brings new ethical problems which are mainly related to issues of media laws
2. To make an indepth study and see if the right of access to information, the right of privacy is threatened by the emphasis on the free flow of information.
3. To study the ethical questions related to technology and its implications on media laws and ethics.
4. To take into consideration various International Conventions and the laws of our land regarding the ethical usage of internet.

Research Question

Is this paradigm shift in this digital age bringing new ethical problems which are mainly related to issues of media laws; such as the right of access to information or the right of privacy?

Research Design

The research is a Descriptive and Diagnostic one. Moreover it will be an exploratory study as not much literature was available on the topic and the study is this field is a new one so we have to explore the possible ways in which we can protect the violation of rights over the digital platform. The data are mainly collected through secondary sources like books, newspapers, magazines and internet sources and primary sources like interviews.

I. Introduction

Definition of digital media:

Digital space is also popularly known as the New Media. These two terms seem synonymous to the Internet and World Wide Web.

Online newspapers, websites, podcasts, bloggers and the like are all examples of new or digital media. But, in reality, the full spectrum of digital space is quite broad and includes a wide host of technology like the wireless and mobile media, satellite radio, digital television, digital music players, digital cameras and other new or emerging technologies for mediated public communication.

John V. Pavlik, in his book, 'Media in the digital age'[1], defines Digital media as, "the system of public communication, the systems of content production and distribution and the computer and network-based technologies that support and shape them. Rather the term 'Digital media' includes all the traditional media of

mass communication including newspapers, magazines, book, radio, television and the cinema which are now undergoing a digital sea change. The term 'Digital media' also includes emerging new media accessed online and through other digital delivery media many of which serve specialised audiences and communities and not a mass audience in the traditional sense."

Definition of ethics:

Stephen J. A. Ward, in his book, 'Ethics and the Media: An Introduction'[2] describes the concept of ethics. Ethics comes from the Greek word 'ethos' meaning character, nature or disposition. The notion is closed to the common idea of ethics as an internal matter of virtuous character that motivates people to act correctly.

The etymology of ethics suggests that ethics is both individualistic and social. It is individualistic because individuals are asked to make certain values part of their character and to use certain norms in decision making. It is social because every person cannot formulate their own rules of what is right or wrong but they have to honour rules of fair social interaction – rules that apply to humans in general or all members of a group.

Definition of media ethics:

Pavlik (2008) mentions that 'in journalism and media ethics usually indicates a set of practices, a code of things that journalists and other media professionals should or should not do. It is a normative concept. These codes are helpful and important but they are not sufficient.'

Transformation of media in the digital age:

Pavlik (2008)[1] mentions that the transformation of media in the digital age involves at least twelve dimensions. They are:

1. The medium of digital delivery;
2. The devices for accessing, displaying, watching and listening to digital media;
3. The audience or users of digital media;
4. The producers of digital media;
5. Digital media content itself;
6. The distributors of media;
7. The financers, owners and business of media;
8. The regulators and law of media;
9. The digital technologies of production (and encryption) that in many ways are fuelling the explosive growth in media production and protection;
10. The inventors and innovators of next generation media;
11. The ethical framework surrounding or providing context for media;
12. The next generation of media consumers, users and creators – children.

II. Digital space vis-à-vis challenges to Media laws and ethics:

Digital platform raise ethical challenges for both professionals and citizens. A few issues that we would be dealing in this paper are:

1. Copyright:

The Copyright Act, 1957[4] (as amended by the Copyright Amendment Act 2012) governs the subject of copyright law in India. The history of copyright law in India can be traced back to its colonial era under the British. The Copyright Act 1957 was the first post-independence copyright legislation in India and the law has been amended six times since 1957. The most recent amendment was in the year 2012, through the Copyright (Amendment) Act 2012.

The development of the Internet industries has brought opportunities for the copyright industry as well as new challenges for the judicial protection for copyright. Copyright law has always adapted to technological change, from its origin in response to the development of the printing press, through the revolution of broadcasting via radio and television, and now the transformation of creative works into digital formats available all over the world via the Internet

Digital technology and networks have had a profound effect on how copyrighted works are delivered to the public. The tools available in the digital environment have changed the nature of what creators are able to produce and how they share their works with the public, and the ways the public can access that content and interact with it.

2. Plagiarism:

Plagiarism is the 'wrongful appropriation' and 'stealing and publication' of another author's 'language, thoughts, ideas, or expressions' and the representation of them as one's own original work.[5]

In the recent years, there is an escalation in the reported cases of plagiarism across various fields in India[6]; popular films were blamed of plagiarism; several scientists and journalists have allegedly faced plagiarism charges.

Plagiarism is an offshoot of copyright violation. With the internet or the digital medium being flooded with information; mainly the open sourced documents, pdfs, power point presentations, blogs, etc.; it becomes very easy for people to copy and paste materials. Thus, most people term 'online plagiarism' as 'online opportunism'.

3. Digital manipulation of photos and videos:

Photo manipulation is a process to transform a photograph into a desired image. Photo manipulation has been regularly used to deceive or persuade viewers, or for improved storytelling and self-expression. Often even subtle and discreet changes can have profound impacts on how we interpret or judge a photograph. Photo manipulation alters the content of the images in a devious manner. It becomes difficult for the audience to differentiate between a manipulated image and reality. There is a growing body of writings devoted to the ethical use of digital editing in photojournalism. In the United States, for example, the National Press Photographers Association (NPPA)[7] have set out a Code of Ethics promoting the accuracy of published images, advising photographers not to manipulate images that can mislead viewers or misrepresent subjects. Infringements of the Code are taken very seriously, especially regarding digital alteration of published photographs.

4. Right to Privacy:

The United Nations General Assembly, in its sixty-eighth session Third Committee Report, reaffirmed the purposes and principles of the Charter of the United Nations; the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights; and also further the Vienna Declaration and Programme of Action, noted that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of Governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern, reaffirming the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his/her privacy, family, home or correspondence, and the right to the protection of the law against such interferences, and recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and one of the foundations of a democratic society.[8]

Digital space vis-à-vis Cyber crimes:

Neelamalar (2010)[4] points out the emerging trend of committing cyber crimes wherein criminals simply devise different ways to undertake standard criminal activities such as fraud, theft, blackmail, forgery and embezzlement using the new media, often the Internet.

Some of the common cyber crimes are:

1. Hacking:

Unauthorized access to a computer network.

2. Cracking:

Causes disruption to a network for personal motives.

3. Virus:

Used by hackers to infest a computer and damage its data.

4. Data diddling:

Involves altering raw data just before it is processed by a computer and then changing it back just after processing is complete.

5. Email bombing:
Refers to sending a large number of emails to the victim that results in the crashing of victim's email account.

6. Phreaking:
Breaking the security of a computer network.

7. Cyber terrorism:
An intentional negative or harmful use of IT for producing destructive and harmful effects to property, whether tangible or intangible, of others.

8. Spamming:
E-mail sent to many unwilling recipients to sell products or services or with the intention of cheating naive customers.

9. Spoofing:
Using the wrong originating address on a TCP/IP packet. A spoofed email will show its place of origin as different from the actual one.

10. Phishing:
Using a forged or spoofed e-mail or website that tricks victims to reveal confidential information that can be used for penetration, financial fraud or theft.

11. Internet pharming:
Redirecting the website used by the customer to another bogus website by hijacking the victim's server and changing the IP address to the fake one to gain unauthorised information.

12. Harassment through emails and SMS:
It is called e-harassment which includes blackmailing, threatening, bullying, abusing with obscene pictures and messages.

13. Cyber stalking:
It is the use of internet to stalk someone. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, blogs, open publishing websites and emails.

14. Cyber defamation:
This occurs when a person defames another through the internet. Eg. someone publishes defamatory matter about an individual on a website or sends emails containing defamatory material.

15. Morphing:
Morphing is editing the original picture and reposting it through fake ids.

Tools for committing cyber crimes:

The following are a short list of tools that are used for committing cyber crimes over the years[9].

1. Bots:
Bot is actually short for robot. Bots are one of the most sophisticated types of crimeware facing the Internet today. Bots are similar to worms and Trojans, but earn their unique name by performing a wide variety of automated tasks on behalf of their master (the cybercriminals) who are often safely located somewhere far across the Internet. Tasks that bots can perform run the gamut from sending spam to blasting Web sites off the Internet as part of a coordinated "denial-of-service" attack. Since a bot infected computer does the bidding of its master, many people refer to these victim machines as "zombies."

2. Keylogging:
A device or software that records keystrokes entered by a user, usually to secretly monitor and/or maliciously use this information. A keylogger is a tool that captures and records a user's keystrokes. It can record instant messages, email, passwords and any other information you type at any time using your keyboard. Keyloggers can be hardware or software. One common example of keylogging hardware is a small, battery-sized device that connects between the keyboard and the computer. Since the device resembles an ordinary

keyboard plug, it is relatively easy for someone who wants to monitor a user's behavior to physically hide such a device in plain sight.

3. Bundling:

Covertly attaching a virus or spyware to a benign or legitimate download, such as a screensaver or a game. When the computer user downloads and installs the legitimate file, they are unwittingly also giving permission to install the criminal program.

4. Denial of Service:

An attack specifically designed to prevent the normal functioning of a computer network or system and to prevent access by authorized users. A distributed denial of service attack uses thousands of computers captured by a worm or trojan to send a landslide of data in a very short time. Attackers can cause denial of service attacks by destroying or modifying data or by using zombie computers to bombard the system with data until its servers are overloaded and cannot serve normal requests.

5. Packet Sniffers:

Software programs that monitors network traffic. Attackers use packet sniffers to capture and analyze data transmitted via a network. Specialized sniffers capture passwords as they cross a network.

6. Rootkit:

A set of tools used by an intruder after hacking a computer. The tools allow the cybercriminal to maintain access, prevent detection, build in hidden backdoors, and collect information from both the compromised computer.

7. Spyware:

Software that gathers information without the user's knowledge. Spyware is typically bundled covertly with another program. The user does not know that installing one also installs the other. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

8. Social Engineering:

Social engineering is not limited to cybercrime, but it is an important element for cyber fraud. Social engineering tricks deceive the recipient into taking an action or revealing information. The reasons given seem legitimate but the intent is criminal. Phishing is an obvious example, a certain percentage of users will respond unthinkingly to a request that appears to be from a legitimate institution.

9. Worms and Trojans:

A trojan is a malicious program unwittingly downloaded and installed by computer users. Some trojans pretend to be a benign application. Many hide in a computer's memory as a file with a nondescript name. Trojans contain commands that a computer automatically executes without the user's knowledge. Sometimes it can act as a zombie and send spam or participate in a distributed denial of service attack. It may be a keylogger or other monitoring program that collects data and sends it covertly to the attacker. Worms are wholly contained viruses that travel through networks, automatically duplicate themselves and send themselves to other computers whose addresses are in the host computer. In the past, cybercriminals occasionally use worms and trojans to hijack a victim's Web browsers. They replace the victims' home and search pages with links to Web spam, as well as drop links to the spam in the victims' bookmarks and on their desktops. To make money, they infect computers with malicious code that generates fraudulent ad views.

10. Virus:

A program or piece of code that spreads from computer to computer without the users' consent. They usually cause an unexpected and negative event when run by a computer. Viruses contaminate legitimate computer programs and are often introduced through e-mail attachments, often with clever titles to attract the curious reader.

11. Internet message boards:

Internet message boards dedicated to stocks are fertile ground for impersonators. A habit of many posters to these boards is to cut-and-paste press releases and news stories from other electronic sources into their posts to alert other posters and visitors to that information. Frequently, posters will paste in a hyperlink to direct a reader to a source directly.

III. Laws for protection of Cyber crimes in India

Information Technology Act 2000 & Information Technology Amendment Act 2008:

There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology 'INFORMATION TECHNOLOGY ACT, 2000' [ITA- 2000] was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. The above Act was further amended in the form of IT Amendment Act, 2008 [ITAA-2008].[10]

The scope and applicability of ITA-2000 was increased by its amendment in 2008.

Though ITA- 2000 defined 'digital signature', however said definition was incapable to cater needs of hour and therefore the term 'Electronic signature' was introduced and defined in the ITAA -2008 as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone.

The new amendment has replaced Section 43 with Section 66. The Word "hacking" used in Section 66 of earlier Act has been removed and named as "data theft" in this section and has further been widened in the form of Sections 66A to 66F. The section covers the offences such as the sending of offensive messages through communication service, misleading the recipient of the origin of such messages, dishonestly receiving stolen computers or other communication device, stealing electronic signature or identity such as using another persons' password or electronic signature, cheating by impersonation through computer resource or a communication device, publicly publishing the information about any person's location without prior permission or consent, cyber terrorism, the acts of access to a commuter resource without authorization, such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc. The offences covered under section 66 are cognizable and non-bailable. Whereas, the consequence of Section 43 of earlier Act were Civil in nature having its remedy in the form of damages and compensation only, but under Section 66 of the Amendment Act, if such act is done with criminal intention that is mens rea, then it will attract criminal liability having remedy in imprisonment or fine or both.[10]

Issues not covered under ITA:

ITA and ITAA is though landmark first step and became mile-stone in the technological growth of the nation; however the existing law is not sufficed. Many issues in Cyber crime and many crimes are still left uncovered.

Territorial Jurisdiction is a major issue which is not satisfactorily addressed in the ITA or ITAA. Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers' powers to enter, search a public place for a cyber crime etc. Since cyber crimes are basically computer based crimes and therefore if the mail of someone is hacked in one place by accused sitting far in another state, determination of concerned P.S., who will take cognizance is difficult. It is seen that the investigators generally try to avoid accepting such complaints on the grounds of jurisdiction. Since the cyber crime is geography-agnostic, borderless, territory-free and generally spread over territories of several jurisdiction; it is needed to proper training is to be given to all concerned players in the field.

Preservation of evidence is also big issue. It is obvious that while filing cases under IT Act, very often, chances to destroy the necessary easily as evidences may lie in some system like the intermediaries' computers or sometimes in the opponent's computer system too.

However, most of the cyber crimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of ITA or the ITAA which gives a comfort factor to the investigating agencies that even if the ITA part of the case is lost, the accused cannot escape from the IPC part.

THE MAJOR ACTS WHICH GOT AMENDED AFTER ENACTMENT OF ITA:

I. The Indian Penal Code, 1860

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC under section 463,464,

468 and 469 read with the ITA/ITAA under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.

II. The Indian Evidence Act, 1872

Prior to enactment of ITA, all evidences in a court were in the physical form only. After existence of ITA, the electronic records and documents were recognized. The definition part of Indian Evidence Act was amended as "all documents including electronic records" were substituted. Other words e.g. 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were also inserted to make them part of the evidentiary importance under the Act. The important amendment was seen by recognition of admissibility of electronic records as evidence as enshrined in Section 65B of the Act.

III. The Bankers' Books Evidence (BBE) Act, 1891:

Before passing of ITA, a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. After enactment of ITA, the definitions part of the BBE Act stood amended as: "bankers' books include ledgers, day-books, cashbooks, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry ...certified in accordance with the provisions ....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data ...to retrieve data that is lost due to systemic failure.

The above amendment in the provisions in Bankers Books Evidence Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out or electronic document is accompanied by a certificate in terms as mentioned above.

IV. Conclusion

After taking an indepth look at all the laws relating to the protection against cyber crimes, we have come to the conclusion that:

1. No Code of conduct manual relating to cyber users have been instituted in India that explicitly mentions all crimes related to digital space.
2. The NGOs along with public should put pressure on the government to take the matter into notice and initiate the process to make all encompassing legislations on the matter.
3. The media should focus on this aspect so that the public at large is made aware of the need for protection against cyber crimes.

References

Bibliography

[1]. Pavlik, John V. (2008). Media in the Digital Age. Columbia University Press, New York.
[2]. Ward, Stephen J. A. (2011) Ethics and the Media: An Introduction. Columbia University Press, New York.
[3]. Neelamar, M. (2010). Media Law and Ethics. PHI Learning private limited, New Delhi.

Websites

[4]. http://copyright.gov.in/
[5]. https://en.wikipedia.org/wiki/Plagiarism
[6]. http://www.academia.edu/12359937/_Thou_Shalt_Not_Steal_Combating_the_Problem_of_Plagiarism_in_Indian_Theological_Institutions
[7]. "NPPA Code of Ethics (dead link)". National Press Photographers Association.
[8]. https://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf
[9]. http://sysnet.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf
[10]. http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective