SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

PERSPECTIVES ON CYBER LAWS AND CYBER CRIMES AND ITS AWARENESS IN INDIA

Dr. Inturu Durga Prasad
Damodaram Sanjivayya National Law University

ABSTRACT

As computer use increased, the cyber world era saw both an increase in technology and an increase in crimes. These days, cybercrime has seriously harmed people, businesses, and even the government also. Cyber law as a major impact in the activities and it covers a large platform of the cyberspace. Cybercrime is increasing in in India primarily because of two reasons i.e., lack of awareness among people and due to lack of proper laws. There is an urgent need for an exhaustive and all comprehensive Information Technology Act to deal with the fast growing problem of cybercrime.

Lack of awareness adds to the increasing problem of cybercrime. The police department and other government departments are not aware of this. Before they can effectively combat cybercrime, police should educate themselves about it. Cybercrime is, broadly speaking, any unlawful activity carried out through or in connection with a computer system or network, including unlawful possession, distribution, or offering of information via a computer system or network cyber laws and cybercrimes, awareness of these issues must be spread throughout public spaces, educational institutions, and universities. In this paper focus on urgent need of laws about cybercrime and legal awareness to public and government police department etc.

KEY WORDS: *Computer, Legal awareness, Network, Police Department*

I. INTRODUCTION

Cybercrime is a term that describes, in broad and varied terms, the various types of crime that involve computers or computer networks. These include crimes in which computers are used or targeted as either the means to perpetuate the crime or as an accessory to the crime. Generally speaking, any criminal activity that occurs in cyberspace, in the online world of the Internet, is a cybercrime. This includes, but is not limited to, the illegal acquisition, manipulation, or destruction of intellectual property. Additionally, cybercrime also includes new types of offenses, such as cyber pornography, information warfare, economic espionage, and a variety of other illegal deeds that are carried out by using technological advancements.

Cybercrime is characterized as borderless; it does not respect geographical or cultural boundaries and, therefore, is a worldwide phenomenon. Through the Internet, cybercrimes can be committed from almost any location at virtually any time. Because of anonymity, it further complicates law enforcement's work in identifying and prosecuting perpetrators.

Among the most perilous cybercrimes that have serious societal implications are child pornography, cyber trafficking, online gambling, and financial crimes.

II. CYBER LAW IN INDIA

[i]As we all know that this is the era where most of the things are done usually over the internet starting from online dealing to the online transaction. Since the web is considered as worldwide stage, anyone can access the resources of the internet from anywhere. The internet technology has been using by the few people for criminal activities like unauthorized access to other's network, scams etc. These criminal activities or the offense/crime related to the internet is termed as cyber crime. In order to stop or to punish the cyber criminals the term "Cyber Law" was introduced. We can define cyber law as it is the part of the legal systems that deals with the Internet, cyberspace, and with the legal issues. It covers a broad area, encompassing many subtopics as well as freedom of expressions, access to and utilization of the Internet, and online security or online privacy. Generically, it is alluded as the law of the web.

Cybercrime is the new global malaise, spreading its domain rapidly across boundaries and affecting societies, individuals, organizations, and corporation's world over. As humans increasingly develop their dependence on digitalization, cybercrimes have proliferated in an equal ratio. Internet, as a medium for information sharing and academic purposes, has evolved into a fulcrum for supporting e-business, e-commerce,

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

India, like any other nation, has identified the imperative need to cope with cybercrime through legislation. As technology advances and internet usage grows, the demand for stronger cyber laws has become a matter of increasing attention. Traditional laws designed for a pre-digital age have proven inadequate in dealing with the challenges posed by the digital age. For instance, lack of legal recognition of email and other online communication systems has left them vulnerable to judicial reluctance, in the absence of specific laws. Such a need for a complete Cyber Law structure has become inevitable.

Cyber law is crucial for the regulation and dealing of any illegal activities carried out in cyberspace. It also offers legal structures to deal with Internet crimes and electronic communication-related crimes. Otherwise, e-commerce, which is among the Internet's most significant upcoming markets, could not be developed and sustainably supported without such law. It is crucial that the proper legal provisions be set in place for the smooth development of digital transactions and that business and individuals should be safeguarded in virtual space.

III. PRESENT SCENARIO OF CYBER CRIME

[ii]With the advent of high-speed internet and mobile technologies, the cyber crime graph is rapidly increasing in our country. In an offline world, people can be advised to refrain from going to lonely places where robbers can snatch the valuables and run away easily. But in the case of the digital world, things are very different so much so that a well-educated gentleman can also become the victim of cyber crime. Every day the news watchers do observe new cases of cyber crimes being reported. Few cases have demanded LEAs to do deep-diving into the cyber world, liaison with cyber and digital experts to nab the culprits. The fundamental idea behind compiling this booklet is to provide LEAs with a glance at emerging cyber crimes in India. The booklet shall also try to present the Modus Operandi of each mentioned case so that those investigation officers who might have not come across similar incidents may also get an overview of the crimes. For the larger benefit of its readers, few emerging cybercrimes being reported outside India are also included. This booklet comprises various verticals of cyber crimes like cyber extortion, Internet Banking frauds, Crypto currency frauds, Dark net frauds and Social Network frauds to name a few. All the cases compiled in this booklet have been taken from reliable news sources, social media and government publications. Since cyber crimes are increasing every day and criminals keep employing new modus operandi, it has been planned that this booklet will be released incrementally.

Cybercriminals have new tools at their disposal and are becoming more adaptive than ever. In the present scenario, advent of technological revolution has given broader opportunities and scope to internet users, but at the same time this has led to the global high-tech cybercrime. In present time every institute of Government sector and private sectors Maximum works depend on internet that's why cyber security awareness should be an important because it encompasses everything that pertains to protecting our sensitive information intellectual property and Governmental information. The impact of cybercrime on societies across the world is immense and consequential. There also exists an upward trend in the cases of cybercrime activates across the world. Cybercriminal have taken advantage of this gap to undermine global efforts.

India witnessed a drastic rise in cybercrime in the year 2024. Latest data indicates that average complaints per day have surged to 7,000 per day, 113.7% more than during the period of 2021–2023 and 60.9% more than the period of 2022–2023. As many as 7, 40,000 cases were logged onto the Cyber Crime portal in the first four months of 2024, and by September 2024, this number went up to 12 lakh. Victims have lost more than ₹120 crores collectively from the cyber frauds alone in the first nine months of 2024. This increase in cybercrimes reveals the growing scale of the issue, with online financial fraud, identity theft, and cyber bullying being some of the most common types of cybercrimes. Most of these scams are operated from outside India, and countries like Cambodia, Myanmar, and Laos have been identified as major sources.

IV. CYBER AWARENESS NGOS IN INDIA

[iii]New line Computer, computer systems and computer networks provide new sophisticated newline tools to carry out traditional crimes. The computer and networks can be both tools and newline targets of the crime. Thus, there is a need that human behavior should be regulated in newline cyberspace. No country can ignore the disastrous consequences of cybercrime. newline However, no meaningful platform has been created by the countries of the world in this newline regard.

There is no denying that technology has transformed modern society, making life easier and convenient. However, this rapid change in technology also brings along the alarming issue of cybercrime. As education and technology go side by side, they create soil for new types of criminal activities. Youths are taking up cybercrimes, with the abuse of digital resources being used to carry out crimes such as data theft, cyberbullying, fraud, and much more. Cybercrime is considered one of the most complex and pervasive challenges of the digital world today. It is highly variable in terms of awareness, based on the individual's environment and access to technology. Urban

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

populations tend to be more aware of cybercrime than rural populations. This is mainly because urban areas are more likely to have access to computers and the Internet, besides having more exposure to media and educational resources. Therefore, city dwellers tend to be better informed about the risks and consequences of engaging in cybercriminal activities.

It is deeply concerning that cybercrime has evolved into a widespread social phenomenon, posing a significant threat to the fabric of modern society. Addressing this issue requires a multi-pronged approach, involving various levels of intervention from families, parents, communities, and public and private organizations. Among the key players in this effort are Non-Governmental Organizations (NGOs), which have a crucial role in raising awareness about cybercrime. NGOs can help disseminate vital information on how to identify and deal with cyber threats, and actively engage with local communities to promote a safer online environment. Through initiatives such as organizing seminars, workshops, debates, and awareness campaigns, NGOs can educate the public on the dangers of cybercrime and the steps individuals can take to protect themselves from digital threats.[iv]

In the light of the alarming rate at which cybercrime is increasing, it is high time that society adopts quick and efficient steps to put an end to this menace. This should be achieved by cultivating awareness and proper usage of the internet, and educating people about the safe use of the digital world.

V. LEGAL MEASURES NEEDED TO TACKLE CYBERCRIME

[v]Usage of internet has become a daily routine for majority of people for day-to-day transactions. The number of internet users has grown tremendously and so does cyber-crimes. Cyber-crime is the crime that is done using computer and network. The threat of cyber-crime is an ever present and increasing reality in both the private and professional sectors. With the advent of internet, old crimes have taken on a new appearance. The purpose of this research is to make awareness regarding cyber-crimes which are happening in today's world and also to create awareness of increased cyber security. This paper attempts to analyze the awareness of cyber-crime among internet users with different age groups and educational qualifications. Linear Regression Model has been applied for analyzing both the objectives. This paper finds that there is a relationship exists between the age groups and educational qualification of the respondents. So, it is the duty of one and all internet users to be aware of the cyber-crime and security and also help others by creating awareness among them. The legal framework plays a vital role in the regulation of cybercrime, especially in the areas of privacy protection and digital security. Laws must be designed to provide assurance to internet users, empower law enforcement agencies, and deter potential criminals from engaging in unlawful activities online. However, the effectiveness of any law depends not only on its enactment but also on its rigorous enforcement.

The rapid spread of cyberspace has ended the notion of crimes having fixed locations, times, or individuals. This has brought with it a whole new set of moral, civil, and criminal wrongs that the traditional laws are not prepared to handle. Most of the time, cybercrime professionals and law enforcement officers lacked the necessary knowledge and tools to effectively deal with these emerging threats. Another reason is that traditional laws are inadequate for the complications of contemporary cybercrimes, whereas new laws take considerable time to be at par with swift changes in the digital world. Additionally, as this is an emerging area, law enforcement agencies do not have many precedents to refer to when they are dealing with cybercrime cases.

These lacunas are met by the Information Technology Act, 2000 (IT Act) of India, which takes into account that new forms of cybercrimes, which had not been defined earlier, should be dealt with through amendments. It thus brings in the most crucial changes in the existing legal structures, including the Indian Penal Code, the Indian.

VI. CONCLUSION AND SUGGESTIONS

Information Technology (IT) continues to evolve, presenting new challenges, particularly in combating cybercrime. In India, cybercrime has become a major issue, with many individuals unaware of the risks and lacking knowledge about cyber laws. Despite growing internet usage, individuals often neglect basic cybersecurity practices, contributing to the rise in cybercriminal activities. Cybercrime is a complex issue, involving both individuals and organized groups using technology for financial or personal gain. While cybercriminals vary in expertise, the growing digital landscape amplifies the problem, especially in a country where legal awareness remains low.

The legal mechanism has to become more responsive towards the emergent cybercrimes, thus more dynamic and detailed in order to combat this evolving threat. Information Technology Act was a very vital step forward; however, that needs continuous update, and even the law enforcing agencies require professional training in tackling cybercrimes. *Suggestions:*

- Update and intensify the Information Technology Act that will include emerging forms of cybercrime and adaptation to the advancement of technology

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

- Intensive cybercrime investigation skill trainings, which should not only include sophisticated tools but cyber forensics for law enforcing agencies
- Holding public educative campaigns informing the public how to handle data and other essential security measures from phishing scams among others.
- Incorporate education in cyber security in schools and create a safer online space right from a very young age for future generations.
- Encourage programs of ethical hacking and introduce rewards for taking up a career in cyber security so that one is well prepared for cyber-attacks.
- Design friendly reporting mechanisms by the citizen, ensuring quick responses by the concerned authority, without further delay for an investigation process.
- Encourage the public and private sectors to collaborate in upholding better digital security standards, share intelligence, and improve collective efforts in combating cybercrime.
- Institute regular cybersecurity audits on both public and private institutions in order to detect vulnerabilities in their defenses so that they may improve on their response to cyberattacks.
- Promote international cooperation with other countries to combat cross-border cybercrimes and share experiences and resources in a unified global response.
- Set up dedicated cybercrime enforcement units within the enforcing agencies and train officers to be equipped for solving the unique problems that digital crimes pose.
- More strict laws are required, and courts should have the authority to prioritize cases involving cybercrime over those involving other crimes. The ineffective enforcement methods are a major issue in the fight against cybercrime. To cope with criminals, stricter laws are necessary, as is undoubtedly punishment. Construction equipment must make every effort to raise public awareness of cybercrimes and take action to reduce cybercrime and related issues.

The mentioned ideas seek to create a more robust structure of battling cybercrime in an effective manner, thus creating a safer virtual world for all.

REFERENCES

[i] *Animesh Sarmah, Roshmi Sarmah etc, A brief study on Cyber Crime and Cyber Law's of India, Volume: 04 Issue: 06 | June -2017, International Research Journal of Engineering and Technology (IRJET).*

[ii] *A Report on Emerging Cyber Crimes in India: A Concise Compilation,National Cyber Crime Research & Innovation Centre (NCR&IC) Modernization Division Bureau of Police Research & Development New Delhi,august 2021.*

[iii] *Srivastava, D K, 2021, Cybercrime in India Challenges and Solutions, http://hdl.handle.net/10603/448897*

[iv] *Cybercrime Magazine, List of Cybersecurity Associations and Organizations, CYBERCRIME MAGAZINE (2018), https://cybersecurityventures.com/cybersecurity-associations/*

[v] ***Anupreet Kaur Mokha, A Study on Awareness of Cyber Crime and Security**, Research Journal of Humanities and Social Sciences, **Vol.8,issue.4.2017,** DOI: 10.5958/2321-5828.2017.00067.5.*