INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 3 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A STUDY ON INEFFECTIVENESS IN ADMINISTRATION SPECIFICALLY TOWARDS CYBERCRIME AND SOCIAL MEDIA

AUTHOR - K.RANJITH, STUDENTS AT SCHOOL OF EXCELLENCE IN LAW, THE TAMILNADU DR. AMBEDKAR LAW UNIVERSITY, CHENNAI

BEST CITATION - K.RANJITH, A STUDY ON INEFFECTIVENESS IN ADMINISTRATION SPECIFICALLY TOWARDS CYBERCRIME AND SOCIAL MEDIA, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (3) OF 2024, PG. 360-366, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract:

This study approaches the ineffective administration in cybercrimes and social media. There are many cyber-crimes are occurring in the present world. It is because of the expansion of technological development, increase in internet usage and administrative incapability in processing a law towards it. The administration is facing difficulties in preventing the population from cybercrime towards legally. Cybercrime includes all type of internet scams and frauds. In absence of strengthened legal administration, makes the criminals to approach the population easily. There should be a strong administrative control to protect the population. Even though there are numerous sections, acts, policies, control mechanisms it is difficult to reduce the crimes in India. A country like India, which has largest population in the world, it is difficult to control but it is the duty of administrative bodies to take proper legal actions to control. A qualitative legal approach was applied in the research to accomplish a research objective. Data are collected from secondary (articles, books, publications, magazines) sources. According to the sources, India has many acts, policies and frameworks to control and prevent the cybercriminals in approaching the population. The implementations are poor and it is not enough for cybersecurity and to compete with cybercrimes. The Indian government is repeatedly formulating policies, improving laws, and finding the steps to reduce the crimes. But the India is facing cyber-attacks regularly. To prevent them, the government should improve technically and technologically. The technology can be destroyed only through technology.

Keywords: *Social media, Cybercrime, IT act, administrative incapability, Legal frameworks*.

1) Introduction:

The emergence of computers has provided new opportunities for criminals. This is a result of the increasing reliance on computers in modern life. Despite the widespread discussion of cybercrimes, there is no distinct category of crime known as cybercrime. Offenses such as fraud and forgery are traditional and are covered by separate laws, such as the Indian Penal Code. However, the misuse of computers and related electronic media has led to the development of various new types of crimes with unique characteristics.

A concise definition of these crimes would be "unlawful acts in which the equipment used to process information, whether a computer or a mobile device, serves as a tool," In India, the Information Technology Act indicates the action in which a computer is used for illegal activities. This type of activity often involves adapting a conventional crime by utilizing computers. Cyber defamation is also considered a cybercrime, occurring when defamation is carried out using computers and/or the Internet. For instance, someone may publish defamatory material about someone on a website or send defamatory information via emails to all of that person's acquaintances. According to the Oxford dictionary, stalking is defined as “pursuing stealthily.”

Cyber stalking entails monitoring a person's online activities by posting messages (sometimes threatening) on the victim's frequented bulletin boards, joining the chat-rooms frequented by the victim, and persistently bombarding the victim with emails. The Information Technology Act, 2000 provides legal recognition for transactions conducted through electronic data interchange and other electronic communication methods, commonly referred to as "electronic commerce."

This includes the use of alternatives to paper-based communication and information storage, facilitating electronic filing of documents with government agencies, and amending The Indian Penal Code, The Indian Evidence Act, 1872, The Banker's Books Evidence Act, 1891, and The Reserve Bank of India Act, 1934, as well as related or incidental matters. The Information Technology Act, 2000 applies to the entire country of India and also extends to any offense or violation committed outside India by any individual.

2) Statement of problem:

1. How do administrative incapabilities hinder the enforcement of existing laws against cybercrime on social media?
2. What specific administrative policies are lacking in the legal frameworks addressing cybercrime on social media platforms?
3. How can existing legal frameworks be revised to better address the administrative incapabilities associated with social media-related cybercrime?

3) Research methodology:

This research utilizes qualitative method research approach to analysis the administrative capability towards cybercrime and social media on legal basis. The doctrinal research method using secondary sources like magazines, journals and newspapers etc...

4) Review of literature:

1. Legal Framework
   - Rao, S. (2020). Cyber Law in India: A Critical Analysis

Analyses the Information Technology Act of 2000 and its amendments, evaluating how effectively it addresses cybercrime.

- Sharma, R. (2021). Understanding the Legal Challenges of Cybercrime in India

Focuses on the challenges of enforcing cyber laws and the gaps in legal provisions.

2. Cybercrime Statistics and Trends
   - National Crime Records Bureau (NCRB) Reports

Annual reports that provide data on the rise of cybercrime in India, highlighting trends and areas of concern.

- Cyber Crime Statistics Report by the Ministry of Home Affairs (2022)

Offers insights into the incidence of various cybercrimes, including their geographical distribution.

3. Impact of Cybercrime
   - Kaur, H. (2020). The Impact of Cyber Crime on Indian Society

Explores the social and economic impacts of cybercrime, including its effects on businesses and individuals.

5) Types of cybercrimes:

As previously stated, the ITAA is considered the primary cybercrime law in India for valid reasons. This amendment acts not only established definitions for numerous cybercrimes not previously covered under the ITA but also outlined procedures for their investigation, trial, and related processes. Additionally, the ITAA specifies that its provisions are supplementary to, and not in conflict with, any other penalties or punishments to which the accused may be subject under different laws, including the Code. The key cybercrimes under the ITA, as amended by the ITAA, are as follows:

Hacking:

A hacker is an individual with advanced computer expertise who utilizes their knowledge to gain unauthorized entry into computer networks. Hacking involves obtaining unauthorized access to a computer, computer resource, or computer network. Globally, hacking has become a widespread issue. In simple terms, it involves accessing a computer or computer resource without the owner's permission. Hacking is subject to punishment under Section 43(a) and 43(f) in conjunction with Section 66 of the ITA. It may also be punishable under Sections 406 (criminal breach of trust) and Sections 426, 427 (mischief), 447 (punishment for criminal trespass) of the Code.

Data Theft:

The idea of ownership has transformed in recent years, with data now being considered a crucial form of "property." We regularly provide a significant amount of personal and professional data to various entities and organizations in our daily lives. Additionally, data can be stored in vulnerable formats such as flash drives, CDs, and microchips, making it susceptible to theft.

While technically data theft does not constitute theft of physical property under the law, the Information Technology Act (ITA) does impose penalties for data theft under Section 43(b) in conjunction with Section 66. Unauthorized copying of data may be considered an offense under the ITA, but it is only classified as theft under Section 379 of the law when the storage device containing the data is also stolen.

Cyber defamation:

Defamation through the use of computers and/or the Internet occurs when someone publishes defamatory content about another person on a website or sends defamatory information via email to the recipient's friends. Sending defamatory content directly to the person is not considered defamation, but if the content is sent to third parties through CC or BCC and tarnishes the recipient's image, it is defamation. Publishing defamatory articles and content on a website also constitutes defamation. Cyber defamation is also known as Cyber smearing.

E-mail spoofing:

E-mail spoofing is a type of cybercrime that resembles identity theft but with minor distinctions. In e-mail spoofing, the perpetrator alters the email address and other components of the email header to create the impression that the email originates from a different source. Therefore, a spoof email appears to come from one origin but actually comes from another. E-mail spoofing is frequently employed for data theft and phishing activities. This cybercrime is punishable under Section 66D of the ITA. Additionally, the provisions of Sections 417 (punishment for cheating), 419 (cheating by personation), and 465 (punishment for forgery) of the Code are also applicable.

Cyber stalking and cyber bullying:

The act of cyber stalking has become increasingly concerning and is the online version of traditional stalking. It involves the unwanted pursuit and monitoring of the victim in the digital realm. Cyber stalking is characterized by repetitive harassment and threatening behavior from the perpetrator using internet services.

Similarly, cyber bullying is a significant issue, particularly affecting children who are the most susceptible targets. It entails intentional and repetitive harm inflicted through the use of computers, cell phones, or other electronic devices. As young people are increasingly active on social media platforms, instances of cyber bullying continue to escalate. Studies suggest that more than half of children who use the internet experience cyber bullying at least once. The Cyberbullying Research Centre reports that over 28% of boys and 40% of adolescent girls have been victims of cyber bullying.

The Supreme Court in the case of Shreya Singhal v. Union of India declared Section 66A of the ITA unconstitutional as it violated articles 19 and 21 of the Constitution. The Court found that Section 66A was so broadly written that it directly impacted the public's right to information. This provision created offenses against individuals who used the internet to annoy or inconvenience others, thereby infringing on the freedom of speech and expression of Indian citizens. Consequently, the Court ruled that Section 66A unreasonably encroached upon the right to free speech and disrupted the balance between such right and reasonable restrictions, making it unconstitutional. As a result, cyber stalking and cyber bullying can now be addressed under Sections 66E and 67A of the ITA. Additionally, Section 354 of the Indian Penal Code (IPC) also covers the punishment for cyber stalking of women, while Sections 292, 292A, 293, 294, 469, 500, 507, and 509 of the IPC may also be applicable to cyber stalking cases.

6) History of model law:

The United Nations Commission on International Trade Law (UNCITRAL) adopted the UNCITRAL Model Law on Electronic Commerce in 1996 to promote the harmonization and unification of international trade law. This was part of UNCITRAL's efforts to eliminate unnecessary obstacles to international trade caused by inadequacies and divergences in trade law. UNCITRAL, comprised of member States from all regions and economic levels, has fulfilled its mandate by creating international conventions, model laws, arbitration rules, conciliation rules, and legal guides over the past twenty-five years. Some of these include the United Nations Conventions on Contracts for the International Sale of Goods, the UNCITRAL Model Laws on International Commercial Arbitration, and legal guides on construction contracts, counter trade transactions, and electronic funds transfers. The United Nations Commission on International Trade Law

The Commission adopted a recommendation on the legal value of computer records at its eighteenth session in 1985. Additionally, paragraph 5(b) of General Assembly resolution 40/71 of 11 December 1985 urges Governments and international organizations to take appropriate action in line with the Commission's recommendation to ensure legal security in the context of widespread use of automated data processing in international trade. It is believed that creating a model law that facilitates electronic commerce and is acceptable to States with diverse legal, social, and economic systems will contribute to the development of harmonious international economic relations. Furthermore, it is strongly believed that the UNCITRAL Model Law on Electronic Commerce will significantly help all States in improving their legislation governing the use of electronic communication and information storage, particularly in the absence of such legislation.

1. Adopts the UNCITRAL Model Law on Electronic Commerce as it appears in annex I to the report on the current session;

2. Requests the Secretary-General to transmit the text of the UNCITRAL Model Law on Electronic Commerce, together with the Guide to Enactment of the Model Law prepared by the Secretariat, to Governments and other interested bodies:

3. Recommends that all States give favourable consideration to the UNCITRAL Model Law on Electronic Commerce when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based forms of communication and storage of information."

7) Information Technology act, 2000

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

8) Information Technology act, 2008

The Information Technology Amendment Act, 2008 (IT Act 2008) has been passed on 23rd December 2008 and received the assent of President of India on 5th February, 2009. The IT Act 2008 has been notified on Oct. 27 2009. Though the IT Act, 2000 technically became law of the land, yet it did not come into operation as section 1 (3) of the said Act specifically stipulated that it shall come into force on such date as the Government may, by notification, appoint.

The IT Act aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and to facilitate electronic filing of documents with the government agencies.

The appointment of the Controller for Certifying Authorities has kicked off the process of licensing of Certifying Authorities in India. It is expected that in a couple of months, Certifying Authorities, duly licensed by the Controller, would begin operations of issuing digital signature certificates in India.

9) Result and discussion:

The major factors which have been a reason for cybercrime in India are:

Individual factor

Administrative factor

These both factors are inter-linked between them. The individual factor prevails first because, the initial point of society starts from the individual. The individual factor determines the society as well. The administrative factor has the close relationship with the society. Mainly, administration is for well-being of the society only. So, the administration has responsibility to safeguard the society but the individual also has the duty to abide the administration.

As per the Indian scenario;

There is a good administration but there is no proper control over it. Why because there is a plenty of acts, policies, ministries, boards to control the crimes but there is no awareness about those laws among the society and individuals. This is the major reason for the development of cybercrime in the country.

10) Suggestions:

After thoroughly reviewing the information from this study, several suggestions have been identified that can help prevent cybercrimes in various ways. Some of the commonly recommended measures are:

1. Implementing a computer security model.
2. Monitoring transactions regularly.
3. Keeping up with regulatory updates related to information technology in different countries.
4. Establishing a high technology crime investigation association.
5. Allocating sufficient staff to communicate with regulatory agencies and assist customers.

Many organizations also opt to conduct regular vulnerability assessments on their systems, which may involve simulated targeted hacking. Depending on the industry, organizations can also seek assistance from CERT-In for recovery, damage control, and the operation of their systems. CERT-In periodically issues advisories recommending measures for parties affected by cybersecurity incidents.

Risk, Control and Prevention of Cyber Security:

In order to maintain anonymity, dignity and availability, digital properties must be secured. Awareness is important for the safety of the human brain, electronic devices, physical media and those in motion.

We will need to rely on three main categories:

1. Risk of cybercrime
2. Monitoring cyber-crime
3. Control & Elimination in cybercrime

1. Risk & Potential of Cyber Crime:

India, the second most populous country globally, relies heavily on information technology in daily life, but no system is completely secure. It is essential to acknowledge that despite safeguards, systems can be compromised at any time, making cybercrime a significant risk. Addressing this threat requires dismantling the secrecy of cyber-attacks, which can lead to interference in cyberspace. This field explores forensic analysis of network attacks and the use of mobile devices. Identifying, collecting, assessing, and tracking information on cybercrime risk is crucial, along with understanding victimology.

2. Prevention of Cyber-Crime:

The implementation of effective techniques for eliminating cybercrime tactics can provide the necessary penalties for cyber-offenders when tried in a court of competent jurisdiction. This can serve as a preventive measure for potential offenders. The Indian IT Act 2000, IT Amendment Bill 2006, and IT Amendment Bill 2008 will also undergo review. It is essential to check the Indian cyber laws of Viz Complete.

3. Control & Elimination of Cyber Crime:

To put an end to cybercrime, it is important to focus on educating users and operators in cyberspace about best practices, protective measures, and gaining knowledge about defense strategies. Understanding the underground hacking technologies used by cyber criminals may take time for defence administrators and managers. It is crucial to center on the mindset of hackers, expose their techniques and tactics, and explore various methods for eliminating cybercrime. Similarly, emphasizing the importance of detection is essential. It's important to note that users are often the weakest link in terms of protection.

11) Conclusion:

The increase in internet users has led to a rise in cybercrime incidents, with various types of cybercrimes occurring on a daily basis. However, many people are unaware of the different kinds of cybercrimes beyond hacking and viruses/worms. It is crucial for individuals to be knowledgeable about offenses such as phishing, defamation, identity theft, and cyber stalking that are associated with the internet. Effectively addressing cybercrime necessitates a comprehensive approach that combines legal, technological, and educational measures to create a safer digital environment. Enacting laws alone is not enough; it is essential to ensure their enforceability through skilled law enforcement agencies. The administration must adapt to the evolving nature of these crimes and establish sectors dedicated to preventing such offenses. Proactive measures, continuous adaptation to emerging threats, and coordinated efforts are crucial for combating cybercrime and ensuring a safer digital environment. These efforts will not only advance the battle against cybercrime but also indirectly impact the economy by creating a safer online environment for market activities and better educating consumers on transaction safety.

12) Reference:

1. "Cyber Crime: Investigating High-Technology Computer Crime" by Robert Moore

   This book provides a comprehensive overview of the techniques used to investigate cybercrimes and the legal considerations involved.

2. "Cybercrime and Digital Forensics: An Introduction" by Michael J. O'Leary

   This text introduces the field of cybercrime and the methods used in digital forensics, including case studies and practical applications.

3. "Cyber Crime: A Reference Handbook" by Barbara T. H. Tan

A detailed guide that discusses different types of cybercrimes, their impact, and preventative measures.

4. "Digital Crime and Digital Terrorism" by Chase Collins

   This book explores the intersection of digital crime and terrorism, examining motives and methods.

5. "Cyber Crime and Cyber Terrorism Investigator's Handbook" by Babak Akhgar and Andrew Staniforth

   Focuses on investigative techniques and the legal framework for tackling cybercrimes.