A R DIGITECH
International Journal Of Engineering, Education And Technology (ARDIJEET)
www.ardigitech.in ISSN 2320-883X, VOLUME 10 ISSUE 04 01/10/2022

THE IMPACT OF CYBERCRIME LAWS ON THE INDIAN BANKING SECTOR AND ECONOMY, AS WELL AS THEIR EFFECTIVENESS

Tannvi Yadav*1,Dr. Karan Singh Yadav*2

**1(Research Scholar, Department of Law, Singhania University, Rajasthan, India*
**2 (Supervisor, Department of Law, Singhania University, Rajathan, India*
*thetanvisingh@gmail.com*1*

ABSTRCT

The banking sector in India has benefited greatly from the rapid growth of digitization, which has raised accessibility, convenience, and efficiency among other factors. However, the industry is now more vulnerable to cyberattacks and illicit activities as a result of this digital shift. Cybercriminals have used technological advancements to attack financial institutions, steal confidential data, and execute fraudulent schemes, causing massive financial losses and undermining public confidence in the system. The challenges here must be resolved by enacting robust and all-encompassing cybercrime legislation that can effectively deter, track down, and prosecute cybercriminals. The legislative framework's ability to adapt to evolving cyber threats and safeguard the financial sector and the economy at large will depend on how well-developed these regulations are. This study's goals are to assess India's current legal framework regarding cybercrime and examine how it affects the nation's financial industry and economy. Identification of barriers: The identification and study of barriers to the implementation of cybercrime laws will be the main topics of this section. These difficulties include issues with jurisdiction, technological advancements, stakeholder collaboration, and capacity building. Policymakers and other stakeholders will be better able to address the challenges that need to be overcome in order to improve the legal system if they have a greater grasp of these issues. The proposed outcome will have policy ramifications that will assist authorities and legislators in formulating and implementing measures to effectively combat cybercrime. It will support future legislative initiatives, regulatory decisions, and cyber security frameworks that aim to safeguard the banking industry and support the Indian economy. By achieving these objectives, this research will support ongoing efforts to combat cybercrime, protect the financial sector from cyber-threats, and preserve the robustness and stability of the Indian economy in the digital age.

KEYWORD: *Cybercrime, Banking sector, Economy, Computer,*

INTRODUCTION

Any wrongdoing that can be prosecuted and punished by the state is considered a crime. Cybercrime makes advantage of computers and internet connections. This offense can be committed in a number of ways. In order to reduce cybercrime globally, we need to act immediately. It is quite alarming that cybercrime is on the rise in India. Being aware of the areas where particular forms of cybercrime are more prevalent in advance would be beneficial. Deliberately destroying their bosses' computers was an early example of cybercrime committed by irate workers against their superiors. As the prevalence of home computers increased, thieves focused on that group. Private information is more likely to be kept on computers by users at home. We also discovered that, in

the 1960s, when computers were still enormous mainframes, the first recorded instances of cybercrime took place. This could now be included in the history of cybercrime. Additional investigation uncovered a long history of cybercrime. Because mainframe cybercrimes were not networked and only a few people could access them, they were all "insider" crimes. This suggests that rather than being considered cybercrime, the attempt to compromise mainframe systems was labeled as computer crime. A few number of people were able to use mainframes because of their isolation. Only in the 1980s did the term "cybercrime" start to be used more broadly than "computer crime." Since Internet access was prohibited in some places (like the US military), this type of crime was different from the cybercrime we confront today. Because of this, criminals were unable to carry out their actions. Because of the widespread use of PCs and networks, the phrase "computer crime" has been superseded by "cybercrime".

This phenomena was first known by a number of titles, such as "crime involving computers," "crime connected to computers," and "crime committed with computers." The term of "high technology" crime was expanded to cover "information age" offenses as digital tools became more widely available. This was done to enable universal usage of digital technologies. The internet allowed people to exchange information digitally, doing away with the necessity for paper records. New concepts regarding criminal activities on the internet arose as a result, including "cybercrime" and "net" crime. Cybercrime refers to crimes that are committed with computers and tools at the same time. Until recently, the term "cybercrime" mostly referred to targeted cybercrime. As a result, we are aware that the rise in cybercrime is associated with people's growing dependency on computers. Cybercrime is the use of a computer to commit or assist in the commission of illegal activity. This includes crimes done through computers. Criminals use electronic ways to get access to computer networks and the data they contain; this is known as "cybercrime." Any illegal behaviour occurring in cyberspace is referred to as "cybercrime". Improper usage of a network or computer. This includes both unlawful possession and the dissemination of private computer information. Any illegal behaviour involving the use of a computer is commonly referred to as "cybercrime". Any illegal behaviour that occurs online is referred to as "cybercrime". This area includes computer hacking and identity theft. The following categories can be applied to them: Within this category are classified online treason against governments, as well as online crimes against non-commercial organizations and individuals. Cybercrime has the potential to provide hundreds of millions of dollars, and compared to other traditional kinds of criminal activity, the risk is significantly smaller. This is so because it is far easier to commit a cybercrime than a typical crime. The frequency of cybercrime is increasing daily and is expanding at a rate of fifteen % every year.

Due to the intricacy of the issue, India loses billions of rupees a year as a direct result of the aforementioned crimes, and there is almost little chance that it can be stopped. Most of the people who commit this crime are never apprehended, and those who are rarely brought to justice. This is due to a lack of trustworthy data, institutional and public interest, and broad public understanding. It is challenging to determine the extent of cybercrime and the harm it does when there is a lack of reporting. Because of this lack of information, it is unknown how much of an impact crime has. It is especially crucial to remember this because participation in these crimes is substantially smaller than in other forms of organized crime. India's crime statistics are extremely lacking in information, and the information that is provided does not sufficiently capture the actual scope of crime or how it affects our day-to-day existence. In many parts of the world, the idea that engaging in illegal acts online might constitute criminal behaviour is still relatively new. Cybercrime is defined in the United Kingdom as "any illegal

behaviour that takes place on or through the medium of computers, the internet, or any other technology" by the Information Technology Act. This is its main significance. In contemporary India, cybercrime has quickly grown to become the most prevalent and harmful form of criminal behaviour. Not only are criminals skilled at remaining undetected, but they also significantly contribute to both domestic and global budget deficits.

E-BANKING

Electronic banking, or e-banking, is a system in which financial transactions are managed using data and computer technology as opposed to human labor. The absence of direct communication between the bank and its customers is one way that e-banking varies from traditional banking services. Banks can provide information and services to their customers via e-banking by utilizing a number of platforms that can be used with a range of terminal devices, including a personal computer and a mobile phone with browser or desktop software, telephone, or digital television. Other terms for e-banking include virtual, home, and cyber banking. Included are ATMs, credit cards, debit cards, smart cards, RTGS, mobile banking, internet banking, and other e-banking services.

THE TYPES AND EXTENT OF CYBER CRIME

Criminal activity is closely linked to many aspects of society. The detrimental effects of cybercrime will always exist in our society, no matter how hard we try to stop it. One would ask how it would be feasible to reduce crime rates in the virtual world, which is far more abstract, immortal, and legally unfettered than the real world, given that we haven't been able to do so in the physical world yet. It is natural to wonder how we would ever be able to regulate something like this if we can't even bring down the incidence of crime to zero in the real world. Since we are still unable to reduce crime in the actual world to a level that is tolerable, this is a problem that has a pragmatic focus. However, crime has evolved over time to take on many forms, proportions, and definitions depending on the history of the civilization in question. There can never be a society without crime since criminal activity is unthinkable in the absence of civilization. This indicates that there is a substantial correlation between the kind of crimes committed within a community and the cultural norms of that society. and remedial measures to keep the peace and keep tabs on criminal activities in the area. All branches of government are part of these establishments, from courts to police to prisons. Technical advancement has not helped the state take control of these new socioeconomic and political issues; rather, it has created more complex situations that are difficult to comprehend and even more difficult to implement the laws that are already in place to solve. This has led to the emergence of new, complex scenarios that are challenging to comprehend and considerably more difficult to apply the existing rules to. Rather than helping the state take control of these problems, it has led to the development of new, complex scenarios that are far harder to comprehend and apply the laws that are already in place to handle. The state apparatus does not have the manpower or resources to adequately combat the current wave of criminal activity.

It's safe to state that throughout the preceding three to four decades, nobody could have anticipated the extent of the revolution brought about by computers. Technology has made life easier, but it has also contributed significantly to the economic, cultural, and social convergence of individuals from all over the world. Thanks to advancements in computing, you can travel anywhere in the world without having to move from where you are right now. These kinds of vacations are now feasible for people because to technological improvements.

People are no longer constrained by time or by the physical boundaries separating them from one another thanks to technological advancements. Nowadays, having access to computers has numerous benefits, but it has also created a jurisdictional issue for the judicial system. Having access to a computer has several benefits in the modern era. Even with these benefits, there are many more advantages to owning a computer in the present era.

MEN REA AND ACTUS REUS DOCTRINE IN CYBERCRIME

Another way to look at this concept is to think of it as "the act that the law seeks to prevent," translated literally into English. For there to be a criminal offense, there must first be either an act committed or an act not committed. Whether the deed was intentional or not, this is still true. The phrase "a guilty state of mind" refers to what is intended by the legal concept of "men's rea," which is "a guilty state of mind." The second essential component of criminal behaviour is the offender's mental state at the time of the offense. The two most crucial elements in determining the seriousness of an offense are the men srea and actus rea, in accordance with the theories of classical crime. This is because the decision to breach the law is typically attributed to these characteristics of criminal activity. This is so because actuarial describes the criminal's acts, whereas men's rea describes the criminal's mental condition. Actus rues is a Latin word meaning "the result of human conduct that the law seeks to prevent." The English translation of this French term is "the act that the law seeks to prevent." An English legal notion known as "Actus Reus" is derived from Latin law. This phrase means "the act that the law" when translated literally into English.

Finding out the hacker's mental state is essential when looking into a computer crime. It's also critical to know if the hacker knew that the access they were attempting to obtain was unauthorized. The hacker does not necessarily need to be targeting a "Particular Computer"; it is okay if they manage to get unauthorized access to "any computer." If "any computer" was the target of unlawful access, that is adequate for this purpose. The hacker does not have to be in possession of a "Particular Computer." It will be much easier to demonstrate that the hacker does not belong there and does not have authority to do so if you are aware of the boundaries of the areas the hacker is attempting to access. If the hacker is unsure of where he is trying to gain access, it will be much more difficult for him to gain access. But when the hacker in issue already has limited power—like in the case of an employee of a company—proving that he or she crossed boundaries while knowing they had been crossed becomes more difficult. It's also difficult to demonstrate that the hacker was aware that his actions were unlawful. Furthermore, it is not possible to prove that he understood he was acting beyond what was appropriate. Furthermore, it's difficult to demonstrate that he realized that going over the limit was against the law. Furthermore, there isn't much evidence to support the idea that he even realized his conduct were against accepted social norms. It is impossible to verify this. The backbone of our economy is the financial sector. The growing number of cybercrime cases has resulted in considerable losses for our economy. By making sure that the relevant laws are appropriately applied, cyberattacks should be prevented. Notifying banks and customers about the risk and necessary safety measures is crucial.

CONCLUSION

The study's intended goal is to provide significant new information and recommendations to stakeholders, policymakers, and pertinent authorities regarding the development of cybercrime laws and their impact on the

Indian financial sector and economy. This is the analysis's desired result. Some of the outcomes that are anticipated based on the analysis include the following: An Examination of Current Cybercrime Laws the present cybercrime laws in India are examined in this paper, along with their advantages, disadvantages, and inadequacies. This assessment will pinpoint the areas that need to be changed in order to improve the legal system and effectively address the growing threat of cyberattacks. Identification of barriers: The identification and study of barriers to the implementation of cybercrime laws will be the main topics of this section. These difficulties include issues with jurisdiction, technological advancements, stakeholder collaboration, and capacity building. Policymakers and other stakeholders will be better able to address the challenges that need to be overcome in order to improve the legal system if they have a greater grasp of these issues. An efficacy study evaluates the success of current cybercrime laws in terms of their capacity to identify and investigate cybercrimes, deter cybercriminals, and convict cybercriminals. The evaluation's findings will shed light on areas where enforcement is lacking and where policies may be changed to make them more effective.

A comprehensive examination of the financial impact cybercrime incidents have had on the Indian financial sector and the economy at large is known as a "economic impact analysis." During the course of this inquiry, prospective financial losses and reputational damage will be valued, along with potential effects on investments, business operations, and economic growth. Suggestions for Improvement: The report will include practical suggestions for strengthening cybersecurity safeguards in the banking sector and enacting more legislation against cybercrime. The study that was done will serve as the foundation for these suggestions. Legislative modifications, stakeholder cooperation, public-private partnerships, capacity-building initiatives, investments in cybersecurity infrastructure and training, and other subjects might all be covered by these ideas. The proposed outcome will have policy ramifications that will assist authorities and legislators in formulating and implementing measures to effectively combat cybercrime. It will support future legislative initiatives, regulatory decisions, and cyber security frameworks that aim to safeguard the banking industry and support the Indian economy. By achieving these objectives, this research will support ongoing efforts to combat cybercrime, protect the financial sector from cyber threats, and preserve the robustness and stability of the Indian economy in the digital age.

REFERENCE

S. A. Khan, M. W. Khan and D. Pandey, “A Fuzzy Multi- Criteria Decision- Making for Managing Network Security Risk Perspective”, Cloud- Based Data Analytics in Vehicular Ad-Hoc Networks, IGI Global, 2020.

M.W. Khan, D. Pandey and S. A. Khan, “Test Plan Specification using Security Attributes”, in ICIC Express Letters, An International Journal of Research and Surveys, Volume- 12, No. 9, 2018.

N.Singh, D. Pandey, V. Pandey and M. W. Khan, “Effective Requirement Engineering Process by incorporating Risk Management Approach”, Solid State Technology, Vol. 63, No.5, pp.814-822, 2020.

Sood, Pallavi & Bhushan, Puneet. (2020). A structured review and theme analysis of financial frauds in the banking industry. Asian Journal of Business Ethics. 9. 1-17. 10.1007/s13520- 020-00111-w.

N. Sharma, D. Sharma, Dhiraj and A. Aggarwal, “Internet of Things and Banking Frauds Friends or Foes? A Study of Indian Public and Private Sector Banks,” Journal of Computational and Theoretical Nanoscience. Vol.17, pp.2596-2604. 2020.

Gorman, L. and Maclean, D. Media and Society in Twentieth Century, Blackwell publishing, 2003.

http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html (Accessed on 6th February, 2016)

http://blog.ipleaders.in/cyber-pornography-law-in-india-the-grey-law-decoded/ (Accessed on 5th February, 2016)

R.C. Nigam, "Law of Crimes in India", Principals of criminal Law, Vol 1, (Asia Publishing House, 1965) 6.

Talat Fatima, Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

J.W.C. Turner, Kenney's Outlines of criminal law (19th Edition University Press, Cambridge 1966) 17. also at Talat Fatima, Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary, 2001, p. 81.

http://cybercrime.org.za/definition (Accessed on 4th January, 2016)

http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 4th January, 2016)

http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 4th January, 2016)

Baumol, W. J. (1990). Entrepreneurship: Productive, unproductive, and destructive. Journal of Political Economy 98(5), 893–921.

North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge: Harvard University Press.

Lewis, A. (1954). Economic development with unlimited supplies of labour. Manchester School of Economic and Social Studies, XXII (May 1954), 139–91.

Chenery, H. B. (1975). The structuralist approach to development policy. The American Economic Review, 65(2), Papers and Proceedings of the Eighty-seventh Annual Meeting of the American Economic Association, 310–316.

Acemoglu, D. (2005). Political economy of development and underdevelopment, Gaston Eyskens Lectures, Leuven, Department of Economics, Massachusetts Institute of Technology, Retrieved from http://economics.mit.edu/files/1064