ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

 ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

Analysis Of Cyber-Crime And Cyber-Attacks During The Pandemic

Authored By-Nirmitee Sable
Savitribai Phule Pune University
Examination of Master of Law (LL.M)

A extraordinary and unusual occurrence, the COVID-19 pandemic changed the lives of billionsof people worldwide and gave rise to what is now known as the "new normal" in terms of cultural norms and how we live and work. In addition to having a profound effect on society and business as a whole, the pandemic created a number of unusual conditions relating to cybercrime that had an impact on both. The pandemic's increased fear raised the possibility that cyberattacks would be successful and coincided with an increase in the quantity and variety of cyberattacks. This study examines the COVID-19 pandemic from the perspective of cybercrime and illustrates the variety of cyberattacks that occurred around the world during the epidemic. To understand the strategy of cyberattack efforts, major world events are analysed and taken into account. The analysis demonstrates how attacks gradually increased in frequency to the point where on some days, three or four distinct cyber-attacks were being reported after what initially appeared to be significant gaps between the first COVID-19-related cyber-attack and the pandemic's initial outbreak in China. The paper then uses the UK as a case study to show how cybercriminals used significant occasions and official pronouncements to meticulously plan and develop their cybercrime activities.

Abstract

While the increased usage of the internet has made life easier, it has also raised the risk of online crimes, particularly cyber fraud. The article focuses on the many difficulties that the State's regulatory systems are currently encountering as it evaluates the applicable Indian laws that are currently in force regarding cyber fraud cases. It also refers to efforts made by the international organisation with regional initiatives to provide the area with cutting-edge information technology and steps taken to control cyber security issues, fraudulent, etc. online activities. Two premises serve as the foundation for this research paper: first, the particular roles and responsibilities of people; second, banking organisations. It is necessary to evaluate and redefine both the police and the government. In the context of the current society norms and practises, the roles of these people and organisations have developed over time and are typically well defined. However, they must be rethought and placed within the new social norms of a networked and cyber-capable society. The second is that cyber law enforcement's regulations and practises need to be clarified and improved because cybercriminals can be anyone, from a youngster or novice
to a skilled software specialist. Similar to someone who develops a cyber domain, a cybercriminal could be anyone who is unaware of the nuances of the cyberspace. This essay examines the rules that govern cybercrimes and makes recommendations for how to change them to better handle current issues.

 ISSN: 2582-6433

Introduction

The essence of information and communication technology is one of profound transformation. When an activity is carried out, it is not done irrespective of the means used to carry out the activity or of the individuals carrying out the action. the method used to carry out the activity, the people doing the activity, and the activity itself. The act of stealing information and subsequentlymoney is carried out in the virtual world or cyberspace when committing a cyber fraud offence, therefore both the medium and the perpetrators have an impact on the crime yet neither can cause it. The internet, also known as cyberspace, is a free place with no restrictions on users, unchecked activity, invisible geographic borders, and unimaginable potential, which creates a lot of opportunity for the commission of online crime or cybercrime. Cyberspace has been transformed into a criminal domain for miscreants to carry out any illegal actions that were previously difficult to carry out physically as a result of cybercrime's evolution from minor annoyances to significant crimes. Internet users and institutions are increasingly and seriously being affected by the scourge of cyber fraud. The complexity for the legal and regulatory authorities to secure fraudsters' conviction is growing due to the difficulties of correlating their virtual identities with their identities in the real world. The prevalence of crime in a given societyexposes its susceptibility to that crime, or to a particular crime whose prevalence has increased.In a digital culture, online and cybercrimes pose a constant and serious risk to the safety and property of people, organisations, and occasionally even the "State" itself. In addition to causing human suffering, the rise in fraud during COVID-19 has also been accompanied by a significant rise in online fraud. The number of phishing websites has dramatically increased in 2020, rising by 350% between January and March. Studies show that the rising instances of URL theft and bogus websites are exacerbating issues in specific industries and market segments that negativelyimpact online customers and consumers, creating a trust deficit. Two categories can be used to categorise cybercrime. Computer-related crimes that can only be perpetrated online fall under thefirst category. Computers or related information technology are aimed at the second group. Manyof the offline products in this category are made possible by information technologies. The second category includes cyber fraud, a subset of cybercrime, where computers or ICTs are essential to the crime and usually entail deception in order to gain financial advantage. The statistics on cybercrime that are now available are highly illuminating as to the scope of the crime and its effects on society. Cybercrime in particular is alarmingly prevalent in Indian society's crime rate. From January 2020, the Ahmedabad Police's "Cybercrime Cell" recorded receiving over 15,300 complaints about financial crimes. India is ranked third among the top 20 countries based on the number of victims of online crimes, according to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Centre (IC3) report for 2019. According to the research, there were 93,796 victims recorded in the United Kingdom in 2019, followed by 3,721 victims in Canada and 2,901 victims in India. The survey also noted that with phishing and similar offences being the most often reported complaint,12 cybercrime cost $3.5 billion in

 ISSN: 2582-6433

losses in 2018. The National Crime Records Bureau (NCRB) documented 27,248 instances of cybercrime in India in 2018 in its 2019 report. The report also notes that in 2018, there were 1,34,546 instances of economic offences, such as forgery, fraud, and deception, followed by 20,456 instances of criminal breach of trust and 1,266 instances of counterfeiting. A significant number of complaints have also been filed on "The National Cyber Crime Reporting Portal," a particular website created by the Ministry of Home Affairs (MHA) for the online registration of cybercrime cases. However, according to some research, there are more cyber scams being committed than are being reported. It is thought that the rise in online activities where people engage without having appropriate knowledge on how to engage in security in the virtual worldis directly related to the rise in cybercrime activity. The data of any cyber fraud will not be represented in the official crime statistics as a result of the incapacity to comprehend cyberspace or the reluctance to report instances of cybercrime. Following the pandemic's emergence, there has been a fundamental shift in how people approach using the internet for business transactions.Every day, a significant number of new netizens—people of all ages, from all socioeconomic origins, with all levels of education and literacy, as well as persons from both formal andinformal economic sectors—use the internet for the first time. According to a report by Statist, the number of internet users in India is expected to rise by about 700 million by 2020, making it the second-largest online population in the world. Due to the rise in online activity and digital transactions, there has been an increase in the use of "Digital Financial Services." In addition, as more people go online, the internet has become a prime target for cybercriminals, including hackers and phishers, which has increased the frequency of their targeted operations. These events may have a chilling impact on how the average person uses the internet since if such high profile accounts with additional security measures can be compromised, how much less secure are normal users' accounts? Every day, these criminals come up with fresh schemes and ruses. Cybercrime cannot be completely eradicated, either, although managing the risks can be aided byunderstanding the methods of commission or strategies used by the cybercriminal. Only until the problem's dimensions are understood and the roles played by different stakeholders in increasing cyber security can the issue be resolved. The following section of the essay examines instancesof cyberfraud around the globe and the typical tactics used in such crimes in an effort to emphasise the seriousness of the issue. Incidents of Cyber Fraud Around the WorldThe ability to commit Cyber Fraud in complete secrecy is one of its distinguishing characteristics. These fraudscan be committed from several jurisdictions, which adds to the perpetrator's anonymity. But according to academics, the majority of fraud incidents originate in West Africa, particularly Nigeria. There have been many cases of cyber fraud, and the victims have suffered significant losses as a result. In February 2016, Bangladesh experienced a very terrible and terrifying occurrence in the history of cyber fraud when US $1 billion was unlawfully moved to various accounts without authorisation from Bangladesh Bank's account at the "Federal Reserve Bank of New York." A small portion of it could be found, but a sizable portion was lost. In the Carbanak,"the hacker organisation steals $1 billion from banks globally," there was yet another infiltration.In the case of the Carbanak bank scam, the system was compromised and the databases were altered to the point where cash could be withdrawn from ATMs without having to connect to bank terminals. The bank and several individual customers lost roughly 900 million dollars as a result of this bank fraud, which persisted for a while. In an increasingly systematic manner, cyber

 ISSN: 2582-6433

scams target not only major institutions and banks but also the general populace. Although the general public is targeted at an institutional level, the impacts are felt at the level of the public, leading to a lack of trust in internet platforms. Between April and September 2014, a hacking event resulted in the compromise of 56 million credit cards. There was a malware assault in this instance involving "Home Depot," and the breach resulted in a loss of almost $62 million. In 2013, the "Target Corporation" was the victim of a cyberattack that stole the data of 10 million credit cardholders.

Hypothesis

1. There is a positive relationship between law enforcement &cybercrime.
2. The identified gaps in the e-banking system are a must for quick repairs.
3. There is lack of awareness and knowledge in people to identify fake emails.

Modality And Techniques For Cyber Fraud

The nature and frequency of crimes are likely to alter dramatically in 2020, making it appear extremely different from past years. In 2020, a different image of crime rates could emerge, which could have an impact on the National Crime Records Bureau's figures (NCRB).

The study could show a substantial decrease in classic crimes like robberies, kidnappings, and abductions as well as incidents of road rage, chain theft, and cell phone snatching, among others, while on the other hand, the prevalence of various cybercrimes could rise. This implies that while the frequency of online or cybercrimes may increase, the number of common crimes committed in the offline form is likely to decrease. According to a study, traditional crime and cybercrime rates are negatively associated, meaning that when traditional crime rates decline, cybercrime rates rise and vice versa. Because individuals are spending more time online and less time on the streets outside of their houses, there has been an alarming increase in cybercrime instances while traditional crime rates have decreased. This phenomenon can be related topeople's changing lifestyles and daily routines. The opportunities have, in a sense, been provided to the cybercriminals instead of the traditional criminals. Today, there is overwhelming evidence of an uptick in online fraud. According to the FBI's "Internet Crime Complaint Center (IC3)" study, fraudsters are not inventing new schemes to con people; rather, they are using old ones very cleverly, which makes it harder to catch them every day. Nowadays, con artists are increasingly inventive in how they defraud consumers of their hard-earned money and they use new methods and procedures. Numerous case studies describe the strategies or ruses used by cybercriminals to cheat people out of their hard-earned money. The following is a list of some of the methods cybercriminals have used to accomplish their goals. There are a tonne of copies and phoney websites that only change the letters. The usage of these phoney websites, also known as fake websites, that replicate well-known websites is becoming a prevalent method used by scammers to trick people into giving over personal information or just to advertise for a product sale. Cyberspace is creating its own illicit markets and means of exchange for carrying out onlinefraud. An incident that happened recently in Australia describes how fraudsters utilised the

 ISSN: 2582-6433

"WhatsApp" messaging app to get users to give up their personal information. The scammers sent messages to a user's contacts using her WhatsApp account, and after receiving the recipient's code, they logged into the recipient's account using a different device to create an impersonation. However, it is only one of many instances where the fraud has shown how much of a risk Internet users are exposed to. According to Australian study, social media usage increased by % during the COVID-19 lockdown, and this coincided with an increase in cybercrime. The data from other nations is not significantly different from this, though. Among the different cyberattack patterns, the most common and widely used technique is the exploitation of social media to deceive consumers with deceptive adverts. Many people are getting emails from fictitious email addresses using the names of their friends, family members, or coworkers asking for money for Covid-19 treatment or other things. Similar to this, there has been a rise in fraudulent calls that seem to be from various government agencies but are actually made by imposters. These calls may also claim to help consumers with a variety of online tasks or with online bill payment.

Individual And Institutional Roles In The Regulatory Framework For Preventing Cyber Fraud

Function of Individual The Internet hides geographical and legal boundaries, giving fraudsters a playground in a borderless realm to completely explore for online achievements. The fraudster is not bound by the laws of the countries where such offences are committed and is free to commit crimes against anyone from anywhere. The question of whether cyberspace and the internet can be regulated by a single legal organisation arises given their worldwide character. An individual plays a very important role in preventing any instance of cyber fraud by contributing methods in the absence of any such power or potential. Netizens who are alert, proactive, and vigilant may prevent fraud from victimising numerous people in the chain in addition to themselves. In the absence of any negligence on its part, a banking institution may not be held accountable if an unknowing consumer or user is the cause of a cybercrime. In "Apple Inc. v. The Superior Court of Los Angeles County," the Supreme Court of California ruled that "consumers should face the risk of online credit card fraud and identity theft." The role of an individual or potential victim cannot be disregarded because his promptness may alter both the fraudsters' and his own faith. In the age of the internet, India's Cyber Security Policy needs a means to safeguard data from being compromised by outside parties. The policy states that "preserving cyberspace is a shared responsibility" and that everyone in cyberspace has a duty to at the very least keep their personal zone safe, which when everyone complies with, results in the security of everyone. With the insistence that the policy may give individuals, organisations, etc. the opportunity to have their own security measures based on their own technical and other requirements to combat the issues and danger, the Indian cyber security policy also placed an emphasis on technology-neutral policy. The notion holds true in the area of cyber frauds. Cyber security policy emphasises that not all attacks require special security measures and that a precautionary defence may lower the risk in many threats even at the individual level. The government now has a responsibility to inform the public about cyber hygiene, safe computing, etc.

 ISSN: 2582-6433

Controlling Cyber Fraud: The Reserve Bank's (RBI) Role In The Regulatory Architecture

Information technology is now an essential component of the banking industry and is used in practically all of its processes. Cyberfraud and internet use raise risk in banking operations while also exacerbating security problems and diminishing public trust in it. Attention must be paid to the rise in financial crimes and online fraud. As a result, "to meet the evolving threat environment, bringing at the most recent international standards relating to the governance of IT, and incorporating information security methods to prevent cyber crime separate from improving independent assurance about the efficiency of IT controls," 85 The Reserve Bank of India established a "Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds" under the direction of its executive director, Mr. G. Gopala Krishna (RBI). This working committee's report, commonly referred to as the "Gopala Krishna Committee Report," was published in January 2011. The "Working Group" made a number of recommendations about business continuity planning (BCP), customer education, cyber fraud, IT governance, information security, IT operations, IT outsourcing, IS audit, and legal issues. The Reserve Bank (RBI) issued guidelines on a number of electronic banking topics, including maintaining information security and risk management to prevent cyber-frauds, based on these committee recommendations. It was noted that the measures recommended for implementation cannot be static and that banks must proactively develop, improve, or modify their policies, procedures, and technologies in response to new developments and emerging concerns. The creation of a "Board" within the banks was suggested by the "working group" for IT governance. The board is entrusted with a number of important duties, including formulating a document for routine administration of IT tasks and approving the IT strategy for banks. The "working group" underlined the value of having an information security management structure that is self- contained and isolated through information security functions and procedures. These processes ought to be in line with "the nature and scale of activities of banks," the degree of IT reliance, and the usage of online channels for product delivery. The working group's focus on IT operations was on identifying dangers and vulnerabilities present in the delivery of business services to clients. The working group recommended conducting periodic risk assessments to find operational vulnerabilities and then putting in place controls that are compliant with legal requirements and flexible enough to accommodate the business environment. Based on the research, the Reserve Bank of India (RBI) requested that banks install 24/7 functional IT security measures. The system needs to be fully operational, active, and continuously updated with the most recent information on new cyberthreats. The banks are instructed to exercise caution when addressing commercial or operational needs and should take a thorough approach to network and database security. The access to these databases and networks should be controlled manually, and there should be a clear mechanism for doing so. These databases and networks should always be shut down if the default requirements are met. Banks were required by the RBI to implement a cyber-security (CS) policy outlining a suitable plan for fending off online attacks. Before receiving the Board's approval, the CS policy should have taken into account the company' level of complexity, the allowed level of risk, and other relevant elements that could have an impact on security, such as management and culture. The larger IT policy and IS Security Policy must be separated from the cyber-security (CS) policy. Customers' data must be kept confidential and accurate, according

 ISSN: 2582-6433

to banks. They must build up and run a Security Operations Center (SOC) to monitor and manage cyber hazards in real-time, and they must maintain constant monitoring through the SOC.

Another important instruction from the RBI to banks is the Cyber Crisis Management Plan (CCMP). The National Cyber Crisis Management Plan (CCMP) and Cyber Security Assessment Framework were introduced by "Cert-In," a national nodal agency that has been in existence since 2004. (CSAF). The Central Government established Cert-In in accordance with section 70B of the Information Technology Act, 2000, and in accordance with the authority granted therein. The four components of a Cyber Crisis Management Plan (CCMP), including I Detection, (ii) Response, (iii) Recovery, and (iv) Containment, should be included. Other instructions include taking proactive steps to stop cyberattacks and quickly identify any intrusions so that you can react, recover, and contain the impact. Banks are instructed to be readyfor threats like "zero-day" attacks, remote access threats, targeted attacks, distributed denial of service (DDoS), ransomware/cryptoware, destructive malware, business email frauds like spam, email phishing, spear phishing, whaling, vising frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password-related frauds, etc. All anomalous cyber-security incidents, whether they were successful or failed attempts, must be reported by banks to the Reserve Bank of India as part of their preparation for cyber security. The indicators of cyber security readiness can also include stakeholders' awareness of cyber security. The banks are required to provide both detailed information on information security incidents, including cyberincidents, as well as summary level information. With the suggested actions that the banks are proposing to implement in order to improve cyber security in their operations, the banks are tasked with the responsibility to report material gaps in controls. A prompt examination and modification of the organisational structure is required to manage the cyber security concerns in banks. For stakeholders, top management, and the board to be aware of cyber security, organisational arrangements and setups are crucial. Cyber security cannot be achieved until everyone in the firm, from the top management to the consumers, is properly trained to handle cyber activities. The RBI, the banks, and the Indian government are all working in this direction. The regulatory framework for the administration of security in banks, however, requires an upgrade. The need for a legal framework to capture and prosecute cybercriminals is a crucial component of the overall cyber security framework, even thoughcyber fraud must be combated by proactive screening and numerous security measures. Cybercrimes can be greatly reduced by having a strong legal framework in place to handlerelated issues and crimes. The management of cyber-related problems and crimes is covered in the next section.

Regulatory Structure A Regular And Massive Kind Of "Interstate Communication" Is Offered By Cyberspace.

where interactions between millions of people across various jurisdictions are straightforward. 95 Because there are no consistent laws governing cyberspace, the complexity caused by this rising frequency cannot be rectified. These various jurisdictions in cyberspace are able to exercise their ability "to establish laws binding on things and all persons within its geographical entity, termeda country," thanks to the "principles of state independence, sovereignty, and territorial integrity."

 ISSN: 2582-6433

Because each country has a separate legal system, there may be a problem with conflicts of laws that prevents a dispute from being resolved or causes a cybercrime or fraud to occur between parties from two different countries. Since combating the spread of cybercrime is beyond the capabilities of individual states, jurisdictional concerns in dealing with the threat of cybercrime have prompted the negotiation of various treaties at the international level. The following section goes through the regional and national measures that have been implemented to combat the threat of cybercrime and cyberfraud.

Regional Programs

Only in 2001, the "Council of European Convention on Cybercrime, 2001," composed of 47 European member states, resolved to establish the first international "Convention on Cybercrime." The convention was prepared in collaboration with the United States, Canada, and Japan. The first global document on crimes committed online, the Convention (also known as the "Budapest Convention") "aims particularly at-

(1) In the domain of cybercrime, unifying the domestic criminal substantive law elements of offences and related provisions

(2) granting domestic criminal procedural law the authority essential for the investigation and prosecution of these crimes as well as other crimes committed using a computer system or electronic evidence,

(3) establishing a quick and efficient system of international cooperation. In 1996, a model legislation on Internet commerce was created as the first international instrument "to foster the harmonisation and unification of international trade law." Many nations based their legal systems on the model law's provisions.

1996's Model Law on Electronic Commerce, as revised in 2008. Every country is facing difficulties from the issue of cybercrimes because there is no worldwide regulation of cyberspace. Therefore, adopting a single criminal law strategy that is comparable to the proposal of "European" states as "European Convention" could aid in the battle against cybercrime. The Asia-Pacific Economic Cooperation (APEC) has 100 measures, among other regional efforts, to combat the cybercrime issues. The economic prosperity of the area is one of the forum's objectives. The APEC Telecommunications and Information Working Group's mission stems from the forum's recognition of information and communications technology (ICT) as a crucial medium/tool for business, commerce, and ultimately economic growth (TEL). In order to carry out its mission, TEL published the "APEC Cyber Security Strategy"102 in 2002. The strategy paper has concentrated on a number of crucially critical topics, including cybercrime legislation, technological and security requirements, public awareness, and training and education. A multi- stakeholder initiative was started in 2012 by the OECD's "Working Party on Security and Privacy in the Digital Economy" with the aim of reviewing the "2002 Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security." The OECD Council endorsed this review suggestion in September 2015108 after being prompted to act by widespread cybersecurity

 ISSN: 2582-6433

events that could have an impact on the economy. 109 The recommendations from December 2019 add to the 2015 recommendation.

Indigenous Law

Cyber fraud is not specifically defined by Indian law. It is challenging to define what cyber fraud is in the absence of a statutory definition. It is impossible to describe cyber fraud by saying that physical fraud becomes cyber fraud when it is carried out online. This definition or description is very vague and incomplete. Cyber fraud differs from traditional fraud in a crucial way. In a real-world fraud, the victim is the one who commits the deception. Cyber fraud relies mostly on the cyber system through which it is being carried out, even though the victims may occasionally be deemed negligent due to their negligence. This distinguishes cyber fraud from traditional fraud. In most circumstances, the system cannot be held accountable for fraud that occurs in the real world; yet, in most high-profile incidents of cyber fraud, some sort of system fault results in the conduct of the crime. The issue that needs to be addressed is whether or not the manufacturer of a cyber-system may be held accountable if the system fails if he failed to issue a warning. Can any social media platform be held accountable for failing to protect user data or allowing links to go through to the victim? As in the physical world, the person who commits a cybercrime, not the middleman, bears responsibility. It is challenging to execute, leaving out instances of negligence or situations when the victim is unsure of how safe the system is. Depending on the actions taken by the fraudster, cyber fraud can be classified. However, the definition also takes into account the degree of fraud victims. Cyber-frauds or cyber-scams are frauds that deceive individuals by using popular communication tools like email, instant messaging, and social networking sites. Due to the fact that it was committed in both the physical world and the internet, many refer to it as a hybrid crime. Cyberspace is growing and expanding at an amazing rate, making it uncontrollable for any worldwide fraud that might be going on. In cyber fraud, con artists devise novel techniques to steal victims' sensitive financial and personal data before using it for their own gain. In the majority of cases, Indian courts use the "Indian Penal Code" provisions in the absence of any statutory definition or concept of cyber fraud. Section 17 of the Indian Contract Act of 1872, which contains the element of intent to deceive, may be used to conceptualise an Indian perspective on fraud. Therefore, fraud is defined as an action or omission that is designed to result in wrongful benefit for one party and wrongful loss for another party, whether via the withholding of information or otherwise. Intentional deception is a component of the definition. This concept is applicable to both contractual issues alone and issues that could result in the formation of a contractual relationship. The Indian Penal Code, 1860, is the current criminal code for cyber frauds and other similar schemes carried out in cyberspace (IPC). Certain fraudulent practises are criminal under sections 403–406, section 409, sections 415–418, section 420, section 463, and section 465 of "The Indian Penal Code, 1860," according to various stipulations. Dishonest misappropriation of property is a crime according to Section 403115 of the "Indian Penal Code, 1860." Criminal breach of trust is defined in Section 405 of the Indian Penal Code, and Section 406 of the same code makes it illegal to dishonestly use or dispose of property, misappropriate it, or convert it in violation of the law. If a public employee, a banker, a merchant, or an agent violates the law by engaging in criminal breach of trust, the section provides an additional penalty under section 409. This section will be applicable when online

 ISSN: 2582-6433

(offline) fraudulent acts are carried out with the assistance of or by bankers, bank workers, those managing account holders' accounts, or anyone else who handles sensitive data or information and then disposes of it.

Indian Penal Code, 1860, Section 415 (Ipc)

Cheating is described as a crime in section 417 of the Indian Penal Code, 1860. When someone deceives others or fraudulently or dishonestly induces someone to deliver any property, etc., theyare committing the crime of cheating. Different types of cheating are subject to higher penalties under various sections of the Indian Penal Code, 1860. This includes impersonation fraud, as defined in section 416. Section 419 outlines the punishment for the offence. When a person intentionally replaces, misrepresents, or cheats by appearing to be someone else, they have committed the crime of impersonation. False calls made under service providers' names, etc. Section 419 of the Indian Penal Code, 1960 prohibits using phoney electronic males or representing oneself as a bank official, customer care executive, etc. on behalf of others (relatives, friends, or coworkers). Section 420 sanctions cheating and dishonestly inducing the delivery of property, whereas Section 418 punishes cheating with knowledge that unjust loss may result to a person whose interest the criminal is required to defend. Section 418 of the IPC is applicable to offences committed by employees or agents because they have access to sensitive information about bank customers and their disclosure could cause them great harm. An exampleof an offence where this applies is ATM fraud, which occurs when bank employees share customer information. Forgery, which is penalised under Section 465 of the IPC, is defined as an intentional act intended to cause harm or damage through the production of fraudulent documents or false electronic records. Cybercrime occurs when people use the internet or electronic devices like computers, smartphones, and social networking sites. It welcomes "The Information Technology Act, 2000" (IT Act) provisions.

The laws that apply are included in sections 43, 66, 43A, 65, 66C, and 66D. If any of the aforementioned acts are carried out improperly on a computer, computer system, etc., Section 43 imposes a penalty and restitution. Anyone who engages in any of the forbidden activities listed is subject to prosecution under this section if they do so without the owner or other person in control of the computer, computer system, or computer network's consent. However, if the same offence is committed dishonestly or fraudulently, the doer will be penalised under section 66 of the Information Technology Act of 2000. Section 43 is a civil wrong. Dishonesty and fraudulence in this context shall have the same meanings as ascribed to them in sections 24 and 25, respectively, of the Indian Penal Code (45 of 1860). 130 Recent filings in the High Court of Judicature in Patna under section 66 and other provisions of the Information Technology Act include case 131. In this instance, the petitioner claimed that up to 87 fraudulent transactions occurred during certain times, but he claimed that he never received a mobile message from the bank, proving that bank staff were complicit in the alleged crimes. The case brought up a crucial question about the accountability of bank officials for failing to notify customers about any such transaction that occurred in their account. If a body corporate is irresponsible in securing dataand any individual suffers a wrongful loss or gain as a result and seeks compensation, Section 43A holds the body corporate liable. The passage has a civil tone. The Information Technology

ISSN: 2582-6433

Act, 2000's Chapter XI provides the provisions governing offences. Identity theft is classified asa crime in this chapter under section 66C. The use of a "electronic signature, password, or any other unique identification feature of any other person" is illegal under this clause. This section applies in all circumstances where personal information, such as a password or other distinctive aspect of identification, is taken by phishing, vishing, smishing, pharming, credit card skimming, etc. The most widely utilised methods for data theft by cybercriminals to perpetrate the crime of cyberfraud include creating a phoney duplicate account or several email addresses in someone else's name. The Delhi High Court voiced worries about the laws' inadequacy to address offences like phishing in case 136, however the court ultimately settled the case and noted." There is no "phishing" legislation in India. A misrepresentation made in the course of business that causes doubt about the email's source and origins and causes significant injury to both the consumer and the individual whose name, identity, or password is misused would be considered phishing under Indian law. If the offended party files a lawsuit, it would also constitute a passing off if it damages or tarnishes the plaintiff's reputation. Making bogus websites is another common tactic utilised over the past few decades.

Section- 66D

imposes penalties for anyone caught using any communication device or computer resource to impersonate someone else in order to cheat. Modification of computer source materials is punishable under Section 651 of the IT Act of 2000. The Punjab-Haryana High Court upheld the trial court's decision in Sanjay Kumar v. the State of Haryana140 and found that the accused had fabricated the electronic document. The Information & Technology Act of 2000's Sections 65 and 66 were found to have been violated in this case, along with the restrictions of Sections 420, 467, 468, and 471 of the Indian Penal Code. As a result, the defendant was found guilty of the charges. Every segment of society uses computers, making them an unavoidable part of daily life. As a result, everyone has equal access to them, which promotes growth and progress. However, the difficulties facing the prosecutors and investigators are considerable. Due to the globalised nature of cyber fraud, investigations can be difficult, and occasionally a specialised agency is required to look into certain offences. These matters are investigated in India by the Central Bureau of Investigation (CBI), which "has the ability and mandate to probe the crime in question, if the Court so directs"141. The CBI is a central organisation with a presence throughout India and connections to Interpol. The court did specify that the complainant's or victim's complaint could not be of a private nature in order for the CBI to conduct an investigation.

For every inquiry, the quantity of fraud registrations is essential. The Indian government established its "National Cyber Crime Reporting Portal" in 2018 to allow citizens to file complaints online. Cyber cells in several locations across the nation have been teaching police officers and government workers on how to deal with situations involving digital security while also raising public awareness as part of this project. As a result, reporting a crime gave the subsequent inquiry a focus.

ISSN: 2582-6433

Lack Of Knowledge On Cyber Hygiene

while being aware bears responsibility since it may infect others if not treated on time, so awareness on the topic may help in minimising the risk of victimisation of that second person. leads to severe digital vulnerabilities and inadequacy of traditional crime reaction. Therefore, it is essential that banks establish a strategy for raising stakeholder awareness so that cyber security issues may be dealt with through preventative measures. Because the infrastructure and procedures to deal with such cases are often insufficient, the majority of cyber fraud events go unreported or, if reported, remain unresolved. Once cybercriminals cross regional boundaries, this chance decreases. It is more difficult to settle the dispute and provide justice for the victims due to the disparities in legal and regulatory frameworks between different countries, as well as the problems with conflicting forums and regulations. Other nations have comparable circumstances. The Bangladesh bank fraud or the Carbanak case, among others, are excellent examples because in most of these situations, only a very small portion of the money lost to cyber crime was able to be recovered. In the majority of countries, including India, cyber security plans are still in their infancy. Although individuals and organisations have begun utilising cyberspace for their operations, there is still a long way to go before the public begins to comprehend the tactics used by cybercriminals and law enforcement agencies begin to have the upper hand over them. The tactics and methods used by fraudsters to defraud people both inside and outside of India have been exposed, and one thing is clear: the primary line of defence should be to delay the payment because the majority of users are not business account holders engaged in financial transactions where payment by a specific date is crucial. If payment isn't made right away, nothing will happen for a few hours or a day. When dealing with suspicious activity, it is best to postpone completion of the transaction and instead report it right away to the authorities.

If prompt action is taken and it is proven that the fault was not self-inflicted or contributing, an indemnification may follow. "Delay in case of doubt" is the operating principle for financial transactions conducted online. For online thieves, the window of opportunity is incredibly small. If they miss this opportunity, they are highly unlikely to return because it will be easier to track their digital footprints if they do. Since they are building consumers instead of money, genuine business payments must supply time. Enterprises, especially small businesses, lack "a comprehensive enterprise-wide approach to fraud control," which has turned into a contributing cause in this situation. Therefore, a company-wide strategy of protection through fraud management policy may help to lower the chance of consumer offences being committed. The laws themselves are still changing and will take time to do so. Cybersecurity can only be achieved if there is a global effort for the same, but managing this global effort would take time because the concerns are amplified not only at the domestic or national level but at the international level as well in the absence of any global machinery to manage the situation. A newcooperation accord is necessary to address the problems of cybercrime. For the purpose of combating cybercrime, collaboration is required. While the law can solve the issues of cybercrime, it must also protect individual privacy. As a result, the law must change to address the challenges while still protecting private.

ISSN: 2582-6433

Conclusion

Cyber fraud's prevalence and effects are now a major issue on a global scale. The exponential rise in astoundingly inventive ways to commit cyber fraud is raising worries among international governments as well as providing enormous and difficult tasks for the investigative apparatus. Geographical borders have never been respected by cyberspace, which has compelled international organisations to develop a single strategy to stop the threat. As the sole treaty to address the problems of cybercrime, the Council of European Convention on Cybercrime, 2001, is still in effect. The issue worsens when the nation fails to make any more attempts. However, regional initiatives by the Organization for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) are being made. reflect the concern of society at large, but the rise of criminal and fraudulent activity in 2020 has revealed the depth of these attempts. Due to the lack of any definitions of cyber fraud under the current legislation, the national investigating and prosecution authorities confront several difficulties. There are countless ways to defraud people, and in this environment, the insufficiency of legislation makes it difficult to tackle cyber fraud. Investigating police look into these crimes in accordance with numerous legal regulations; yet, because there are no severe penalties, fraudsters are able to commit these crimes with no restraint. Cyber fraud cannot be defined in a straight-laced manner, and attempting to encompass all instances in one definition is not only challenging but also impossible because certain wrongs are of a private nature and committed against private individuals while others have an impact on the general public. It is necessary to update the Information Technology Act, 2000 to include a chapter on cyber fraud with various requirements for various acts. Additionally, it is necessary to include provisions for the liability of intermediaries in certain financial situations, which calls for an amendment to the IT Act, 2000. However, in the absence of such regulations, public awareness campaigns may be the most effective means of averting victimisation. The Reserve Bank of India periodically issues instructions to financial institutions and recommendations to individuals about how to keep their money safe, lowering the likelihood that cyberfraud would be committed. Banks must closely adhere to RBI advice while being unwavering in how they carry out their obligations to banking clients. With the laws on cyber fraud, policy and planning are crucially needed to raise knowledge about ways and processes to avoid falling victim to cyber scams since a more watchful publican reduces the danger of cyber crime.