CYBER LAWS & INTELLECTUAL PROPERTY RIGHTS

Chandrashekhar
Sakshi Pande
Poojyashree Kumawat

ALEXIS PRESS

CYBER LAWS AND
INTELLECTUAL PROPERTY RIGHTS

CYBER LAWS AND INTELLECTUAL PROPERTY RIGHTS

Chandrashekhar

Sakshi Pande

Poojyashree Kumawat

ALEXIS PRESS

Published by: Alexis Press, LLC, Jersey City, USA
www.alexispress.us

First Published 2022

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication Data

Includes bibliographical references and index.

Cyber Laws and Intellectual Property Rights by *Chandrashekhar, Sakshi Pande, Poojyashree Kumawat*

ISBN 978-1-64532-422-5

CONTENTS

CHAPTER 1

CYBER LAW'S EMERGING ISSUES

Chandrashekhar, Assistant Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- chandrashekhar792@gmail.com

ABSTRACT:

Today, everyone is going towards the era of digitalization and networking, which has several advantages in industries such as e-commerce, communication, and so on. It also gives rise to a new criminal class all of a sudden. Cybercrime is the overall term for this approach. Stopping crimes in such a virtual environment requires a spotlight. On connected laws and orders, it is necessary. There are several options. Rules and regulations that have been drafted and implemented taken to avert catastrophic calamities, such as the IT ACT National Cyber Security Policy, etc. Although the term "cybercrime" does not have a definition or a reference. Point of law, as well as acts such as cybercrime Cyber-vandalism, cyber-violence, and cyber-rape, are not acceptable. Cybercrime is classified and has legal standing. The major focus of this study is on the issues that are now being faced. Internet, emphasizing the pressing necessity for India's cyber edict framework needs to be reformed, and several difficulties that cyber law enforcement lacks.

KEYWORDS:

Cyber Law, Cybercrime, Security Policy, E-commerce, Communication.

1. INTRODUCTION

In terms of technical growth, it is swiftly advancing in a very favorable direction all over the world. However, there are a few drawbacks to this. In the foreground,one of the factors is the rapid expansion of the economy. The use of digital and network technologies aided in the development of constructing a cyberspace virtual world Cyber Every aspect of existence is impacted by space, and this trend is expected to continue. However, there is a simultaneous rise in the economy. Cybercrime is a new type of crime. The internet was originally designed as a tool for study and information sharing, but it is today used by both the target and the perpetrator to perpetrate cybercrime. Communication, e-commerce, and e-governance got increasingly transactional as time went on. Cyber laws include all legal concerns about digital crime.

As the frequency of cybercrime incidents such as unauthorized access and hacking, Trojan assaults, virus and worm attacks, and denial of service attacks rises, so does the demand for corresponding laws and their implementation.Cybercrime has neither a legal genesis nor a legal reference. In a workshop devoted to the concerns of crimes connected to cyberspace during the tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, cybercrime was classified into two categories and characterized as follows.

(a) In a broad sense, cybercrime refers to any illicit activity carried out through electronic means to compromise the security of computer systems and the data they handle.
(b) Cybercrime in a broader sense, includes any criminal action done via the use of a computer system or network, such as illegal possession or distribution of information

through a computer system or network. Attacks against digital networks to gain control or perhaps destroy infrastructures that are key to governments and sectors are of critical relevance from a tactical standpoint.

According to the Norton analysis, cyber assaults against Indian assets are on the rise, with both government and commercial infrastructure being targeted. The government released a national cyber security strategy in July 2013, and it was only a few months later that it was revealed that government officials' emails had been stolen. The NCSP is far from being able to address all aspects of the cyber threat. It just gives guidance for the standard operating procedure and does not leverage its potential for maximum advantage. There is a critical issue of security concern in the telecom business, which is integrated into cyberspace.

As per the strategic viewpoint, assaults on computerized networks to hold onto control or even obliterate frameworks that are essential to legislatures and areas are of critical significance. As indicated by the Norton report recurrence of digital assaults on Indian resources, with the government and private framework similarly overstated. In July 2013 government distributed a public network safety strategy and soon after that it was accounted that administration of the official's messages had been hacked. The NCSP is a long way from noting all sensitivitiesto digital danger. It doesn't expand its potential for the ideal advantage it simply just gives rules for the standard working methodology. The significant place of safety concern connected with the telecom industry which is completely incorporated into the internet is missing.In this, a consistent expansion in the number of such violations in this region is normal which requests for more noteworthy consideration of legislators.

The advancement of technology has increased criminal activity, and the IT Act of 2000 establishes procedures for dealing with cybercrime. This strategy has certain advantages in terms of e-commerce, but it does not fix all of the difficulties and issues fast [1]. The IT Act is seen as a hazy statute since the scope of jurisdiction in the context of the Internet is uncertain. Computer forensics is gaining importance in the field of cyber-crime evidence investigation because, while evidence is tangible in the real world, it is difficult to expunge information from a computer system in the virtual world of cyberspace. To handle this, computer forensics requires an efficient and knowledgeable computer expert because any carelessness leads to the loss of evidence [2]. Even though the IT (Amendment) Act 2008 addresses new issues, the IPC does not utilize the word "cyber-crime" at any time. After the year 2008, there has been a surge in cybercrime as criminals find loopholes in the law and use them to carry out illicit actions. Cybercrime can be committed against people, property, or the government [3].

There are few judicial precedents to go to, and prior statutes didn't quite match the crime at hand. There is a pressing need to enforce cyber laws. Our system should include harsh penalties to serve as a deterrence to future illegal activities [4]. The IT Act (amendment) of 2008 broadened the scope of cyber legislation. The defining section of the Evidence Act has been changed [5].The question of territorial jurisdiction is a key one that the IT Act of 2000 does not adequately address. It is commonly seen that investigators avoid taking complaints based on jurisdiction [6]. India's development has not been realized in all aspects, including E-courts, online dispute resolution, effective cyber legislation, cyber forensics, and so on. The Information Technology Act necessitates being updated. In addition, scientific and technological professional training for lawyers should be made available in India [7].Cybercrime is an emerging trend of crime that has the potential to disrupt every part of society since it is simple to perpetrate but extremely difficult to identify and find in terms of jurisdiction, given the geographical indeterminacy of the internet [8]. To defend the developing ICT, Cyber Security is required. The expert panel should identify and suggest a

good mix of solutions for important ICT systems that support the nation's governance framework [9].

Understanding the cyber threat and creating offensive capabilities in this cyber realm is a must. Nations, non-state actors, terrorists, organizations, and people are all posing a threat to progress, which is becoming increasingly reliant on the cyber domain, necessitating the identification of technology in this area [10].

An enemy is a person who conducts a wicked act. Outsiders and insiders may both be adversaries. Insiders are not the same as outsiders. An insider is a person who has been granted access to a nuclear site or other sensitive operations. They were praised for their authority, which included the ability to get admission. Cybercrime is a multibillion-dollar problem, and to realize the full potential of the computer era, appropriate legislation is required to prevent overshadowing[11].

Governments and businesses all across the world are concerned about cyber security. Cyberthreats can take the form of cyber-attacks, but they can also occur as a result of "mistakes" or natural calamities. As a result, in the context of cyber security, there should be a customized approach to the specific problem. From all of this, it is apparent that a slew of issues must be addressed, including cyber security and a legal framework that covers a wide range of issues such as cloud computing, social media fraud, and scams, among others.

3. CYBER LAW

In 1996, UNCITRAL, the United Nations Commission on International Trade Law, published the United Nations Modern Law of Electronics Commerce, which marked the beginning of the creation of cyber laws in the twentieth century. It was recognized there that the focus of legal provisions should be on users, enforcement agencies, and criminal deterrence, because the person responsible for the misuse of technology, not the technology itself, bears responsibility for the crime. This went on to demonstrate for the first time that it is critical to recognize that the crime is committed by a human rather than a machine or technology. Following this, the UN General Assembly recommended that each state consult the UNCITRAL Model Law in the formation of Cyber Laws.

Following the UN General Assembly's proposal, the Indian government has accepted the necessity to legislate following the UNCITRAL Model Law. As a result, the Information and Technology Act of 2000 was drafted and implemented. The Indian Penal Code was amended as a result of the adoption of the IT Act 200. (e.g. 192, 204, 463, 464, 468 to 470, 471, 474, 476 etc.) Major developments were recognized, such as the acknowledgment of electronic evidence and the management of electronic records and documents. Only tangible evidence and paperwork had legal standing before this. In a nutshell, the legislation covers the following topics:

(a) Legal identification of Electronic documents.
(b) Legal identification of Digital Signatures
(c) Offenses and Contraventions Justice
(d) Dispensation Systems for cybercrimes.

The IT Act of 2000 tries to align the legal system with the needs of the cyber era, and it also addresses the issue of cybercrime in the context of the country's limited e-commerce potential. It takes a risk in attempting to establish an infrastructure that supports the conduct of e-commerce by providing legal underpinnings such as electronic signature recognition. However, the Act does not exempt uncertainty in certain areas, such as internet jurisdiction.

Section 1 (2) states that the act applies to all of India, as well as any office or violation thereof conducted outside of India by any person.

3.1.Various issues under Cyber Law enforcement.

3.1.1. Issues with the legislature

The reference to territorial jurisdiction in sections 46, 48, 57, and 61 about the adjudication process and the procedure in connection with it fails to offer sufficient clarification. Furthermore, section 80 provides a police officer the authority to enter a public location and search for cybercrime. Because cybercrime is a virtual occurrence, such a law causes a lot of uncertainty. In the event of a cyber-attack from one state to another, the legislature remains silent, resulting in a great deal of jurisdictional uncertainty. Furthermore, the IPC ignores even simple phrases like "cyber-crime" throughout its length.

A virtual crime has digital evidence that is harder to identify, extract, and interpret than a physical crime, which has tangible evidence that is comparably easy to detect and make sense of, such as a murder weapons, fingerprints, and so on. To gain entry to such an event, a team of specialists is necessary. The IT statute makes no provision for this essential body of experts. According to a study by the National Crime Records Bureau, 4231 incidents of cybercrime were reported under the IT Act and the IPC in 2009-11, with 1184 people arrested. This emphasizes the necessity for a group of cyber forensics specialists.

To effectively combat cybercrime, there is a need for upgrading technological hardware and software in addition to cyber forensic professionals. Because of this, when the global cyber-attack known as the "wannacry" attack hit India, the country's national security was jeopardized. Because there are no clear standards in this area, telecom businesses have been able to handle user security ineffectively as a result of the loose set of regulations. This is thought to be the main reason for the rise in cyber-attacks, especially those on mobile devices. Furthermore, unlike other regulations, the policies that were approved just serve as suggestions for normal operating practice and have no legal authority. As a result, it is possible to conclude that NCSP has limited potential and advantages.

Another difficulty is that regulations are not evolving at the same rate as cybercrime. Cloud computing attacks, for example, and Denial of Service attacks go unaddressed. This is particularly problematic now that services such as e-locker services via banks, online police records, and private papers, online records of personal documents and personal data, and so on have become available.In the years 2010, 2011, and 2012, 1322, 2213, and 3477 instances were recorded, respectively, whereas only 1191, 1630, and 2071 people were arrested. This proves the law enforcement organizations' inability to catch the offenders, providing concrete proof of all the previously discussed difficulties.In the years 2010, 2011, and 2012, 1322, 2213, and 3477 instances were reported, respectively, whereas only 1191, 1630, and 2071 people were arrested. This proves law enforcement organizations' inability to catch criminals, offering concrete proof of all the previously discussed difficulties.

3.2.A suggested solution to the situation

The Information Technology Act of 2000 is a paper tiger that desperately needs to be strengthened. To begin with, the IT Act (Amendment) Act 2008 significantly decreased the severity of penalties for a wide range of cyber-crimes; this has to be addressed, and a large portion of cyber-crime should be made a non-bailable offense. This will be done to create a deterrent impact in the minds of the criminal population. Furthermore, the Act must be thoroughly revised to include all current terms and types of cybercrime.

The uncertainty around jurisdiction should be resolved to improve the enforceability of cybercrime laws. In all business sectors, including the telecom industry, appropriate and strict norms and procedures should be implemented to secure user data.

According to the 52nd report published by the standing committee on Information and Technology, the statistics on the rate at which the government websites were hacked in inclusion with other websites are (Figure 1):

Figure 1: Data over website hacked in 2008-2013 (1 unit = 10000 websites)

The data in Figure 2 illustrate that cyber-attacks are becoming more common, and not just on commercial websites. In 2008, 6310 websites were hacked; in 2009, 12161; in 2010, 20701; in 2011, 21699; in 2012, 27605; and in 2013, there were just 12693 attacks until June. The graph below, however, illustrates the amount of government websites that were hacked between 2008 and 2013, to demonstrate the problem.

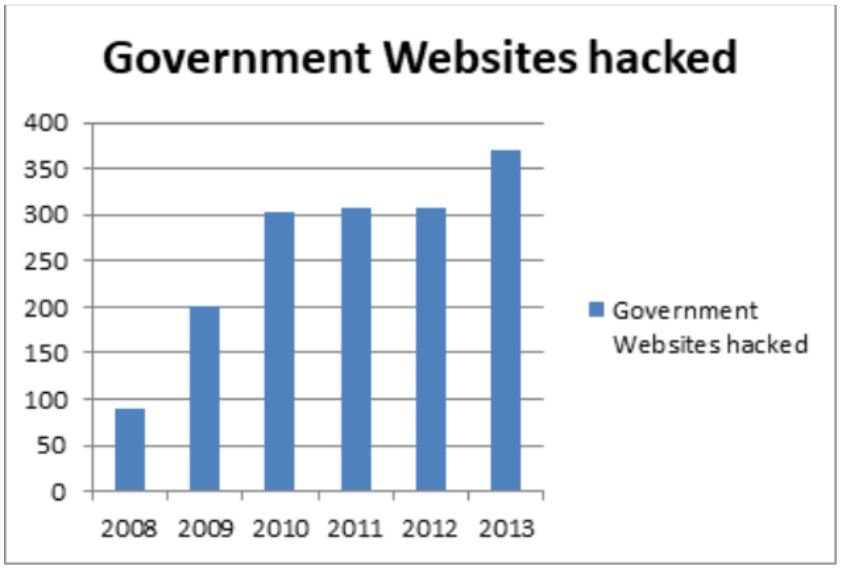

Figure 2: Data over government website hacked in 2008-2013 (1 unit = 1000 websites)

According to the following graph, the number of cyber assaults on government websites is increasing at the same steady rate as commercial websites. From 2008 to 2013, the total number of cases was 90,201,303,308,308,371 (as of June). At this rate, if the problem is not handled, it has the potential to become a national catastrophe, endangering India's national security.

3.3.United Nations Definition of Cybercrime

Not only does cybercrime cut over state lines, but it also cuts across national borders. Perhaps we should appeal to international bodies for a uniform definition of the offense. In a workshop devoted to the challenges of crimes involving computer networks during the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, cybercrime was divided into two groups and characterized as follows:

3.3.1. Cybercrime (computer crime) in its broadest sense:

Any criminal activity directed through electronic operations threatens the security of computer systems and the data they handle.

3.3.2. Cybercrime (computer-related crime) in a broader sense:

Any criminal action performed by or about a computer system or network, including offenses such as illegal possession [and] providing or distributing information via a computer system or network. These definitions are muddled by the way that a demonstration might be unlawful in one country yet not in another.

There are more substantial models, including

i. Unapproved access
ii. Damage to PC information or projects
iii. Computer damage
iv. Unauthorized capture of correspondences
v. Computer surveillance

These definitions, albeit not authoritative, do give us a decent beginning stage that has some worldwide acknowledgment and arrangement for deciding exactly what we mean by the term cybercrime. In Indian law, digital wrongdoing must be deliberate and tenacious, a demonstration or oversight that unfavorably influences an individual or property. The IT Act gives the spine to online business and India's methodology has been to check out e-administration and internet business principally from the limited time viewpoints taking a gander at the huge chances and the need to sharpen the populace to thepossibilities of the data age. There is a need to take into thinking the security angles.

In the present worldwide circumstance where digital control components are significant, we want to push digital laws. Digital Crimes are another class of wrongdoings to India quickly extending because of the broad utilization of the web. Getting the right lead and making the right understanding is vital in tackling digital wrongdoing. The 7-phase continuum of a criminal case begins from execution to enrollment to detailing, examination, indictment, arbitration, and execution. The framework cannot be more grounded than the most fragile connection in the chain. In India, there are 30 million police officers to prepare separated from 12,000 in number Judiciary. Police in India are attempting to become digital wrongdoing-wise and recruiting individuals who are prepared nearby. Each police headquarters in Delhi will have a PC soon which will be associated with the Head Quarter. The speed of the examinations anyway can be quicker; legal affectability and information need to improve. The Center should be around instructing the police and locale legal executive. IT Institutions can likewise assume a part around here.

Innovation subtleties are significant in a spam-plagued climate where security can be compromised and people can be exposed to turning into a casualty accidentally. We want to sharpen our examiners and judges to the subtleties of the framework. Most digital

lawbreakers have a partner in reality. Ifa deficiency of property or people is caused the criminal is culpable under the IPC too. Since the law authorization organizations observe it is more straightforward to deal with it under the IPC, IT Act cases are not getting announced and when revealed are not managed under the IT Act. An extended and concentrated course of learning is required.

An entire series of drives of digital legal sciences were attempted and digital law methods came about out of it. Here learning happens each day as we are for the most part fledglings around here. We are searching for arrangements quicker than the issues can get developed. We want to move quicker than the hoodlums. The main problem is how to forestall digital wrongdoing. For this, there is a need to raise the likelihood of fear and conviction. India has a law on proof that thinks about acceptability, validness, exactness, and culmination to persuade the legal executive. The test in digital wrongdoing cases incorporates getting proof that will stand examination in an unfamiliar court.

For this India needs all-out worldwide collaboration with specific organizations of various nations. Police need to guarantee that they have seized precisely what was there at the location of the crime, the very that has been broken down and the report introduced in court depends on this proof. It needs to keep up with the chain of authority. The danger isn't from the insight of crooks but from our obliviousness and the will to battle it. The law is stricter now on creating proof particularly where electronic archives are concerned. The PC is the objective and the instrument for the execution of wrongdoing. It is utilized for the correspondence of the crime like the infusion of an infection/worm which can crash whole organizations.

The Information Technology (IT) Act, of 2000, determines the demonstrations which have been made culpable. Since the essential target of this Act is to establish an empowering climate for business utilization of I.T., certain exclusions and commissions of hoodlums while utilizing PCs have not been incorporated. With the lawful acknowledgment of Electronic Records and the corrections made in the few segments of the IPC vide the IT Act, 2000, a few offenses having to bear on the digital field are additionally enlisted under the fitting areas of the IPC.

3.4.Threat Perceptions

The United Kingdom has the most infected computers in the world, followed by the United States and China. Financial assaults had the greatest rate of incidents per 1000, at 16 per 1000. The United States is the most common source of assaults, however, this is decreasing. China is in second place, followed by Germany. It's difficult to say where the attack originated from in the first place.

The number of virus and worm variants increased dramatically to 7,360, a 64 percent rise over the previous reporting period and a 332 percent increase year over year. There are 17,500 different Win.32 virus variants. Threats to sensitive data are on the rise, with 54 percent of the top 50 companies reporting malicious code that might reveal such data. Between July and December 2004, the number of phishing emails increased from 1 million to 4.5 million.[12]

CONCLUSION

For the arising pattern of cybercrimes, it is essential to have a cyber-law enforcing energy because digital wrongdoing has the forthcoming to obliterate every single part of life as it is not difficult to carry out yet it's truly difficult to distinguish. However, India has an extremely

gritty and clear-cut general set of laws yet every one of the current laws set up in India was ordered way back remembering the important political, social, financial, and social situation of that applicable time. No one then, at that point, could truly imagine the Internet. Regardless of the splendid ability of our lord designers; the necessities of the internet could scarcely at any point be normal. In that capacity, the happening to the Internet prompted the rise of various touchy legitimate issues and wrongs which required the ratification of Cyber laws. Secondly, the law existing even with the liberal examination couldn't be deciphered at the center of arising the internet. Web requires a steady legitimate foundation in agreement with time. This legitimate foundation must be given by the establishment of the applicable Cyber laws as the current laws have neglected to contribute the same. All these thoughts made empowering climate for the requirement for sanctioning important digital laws in India.

REFERENCES

[1] Maneesh Taneja and Dr. D.B Tiwari, "Cyber Law,International," vol. 11 (21), 2010.

[2] Yougal Joshi and Ananda Singh, "'A Study of Cyber Crime and Security Scenario', vol.3 (3) June, 2013," *Int. J. Eng. Manag. Res.*, vol. 3 (3), 2013.

[3] Ravikumar S. Patel and Dr.Dhaval Kathiriya, ""Evolution of Cybercrimes in India," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 2(4), no. July-August, 2013.

[4] "Cyber Law and IT Talwant Singh, "CYBER LAW and IT."

[5] Rohitk.Gupta, "'An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective,'" 2013.

[6] Rohit k Gupta, "'An Overview of Cyber law vs. Cybercrimes,'" vol. 2013.

[7] Prabhat Dalei and Tannya Brahme, "'Cyber Crime and Cyber law in India: An Analysis,'" *Int. J. Humanit. Appl. Sci.*, vol. Vol.2 (4), 2014.

[8] Aashish Kumar Purohit, "' Role of Metadata in Cyber Forensic and Status of Indian Cyber Law,'" *Int. J. Comput. Technol. Appl.*, vol. 2(5), no. Sept-Oct, 2011.

[9] M. P. G. and J. B. M.M.Chaturvedi, "'Cyber Security Infrastructure in India□: A Study.'"

[10] "IDSA Task Report, 'India's cyber security challenged,'" 2012.

[11] Angshuman Jana and Kunal Kumar Mondal, "'A survey of India Cyber Crime and Law and its prevention approach,'" *'International J. Adv. Comput. Technol.*

[12] "CyberLaw & Information Technology.pdf." .

CHAPTER 2

CORPORATE SOCIAL RESPONSIBILITY EVOLUTION

Pradip Kumar Kashyap, Assistant Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- pradiprgnul@gmail.com

ABSTRACT:

Corporate social obligation (CSR) is a popular expression around the world. In the present globalized world, one of the extraordinary difficulties looked by firms is a reconciliation of CSR in business. Partners require a parcel more from organizations than only seeking development and benefit. CSR has come a long way in India and other developing business sectors. From responsive exercises to reasonable drives, corporates have shown their capacity to have a critical effect on the general public and work on general personal satisfaction. This paper centers on the idea of CSR, its aspects, and its importance in developing business sectors with exceptional reference to India. The idea of Corporate Social Responsibility (CSR) isn't new in India. It arose out of the 'Vedic period' when history was not recorded in India. In that period. Aristocrats committedto society and vendors showed their business obligation by building Places of worship, education, and wells. Corporate Social Responsibility has been characterized and conceptualized in more ways than one during the beyond four centuries following a course of examination, and insightful showdown around the topic. The idea of 'Corporate Social Obligation' (CSR) alludes to a 'delicate', intentional self-guideline embraced by firms to improve parts of the organization, this can connect with work, ecological and basic liberties issues.

KEYWORDS:

CSR, Sustainability, Philanthropic approach, Stakeholders.

1. INTRODUCTION

The notion of corporate social responsibility (CSR) has gained traction in business reporting. Every company has a CSR policy that requires them to prepare an annual report documenting its efforts. Every firm can distinguish between socially responsible and non-socially responsible corporate actions. There are two intriguing aspects to consider in this regard. To begin with, people do not always agree on what constitutes social responsibility. When asked to define anything, even if one claims to know what it is or is not, it is usually difficult. The broadest definition of social responsibility is concerned with the interaction that exists or should exist between global businesses, national governments, and individual individuals. The link between the company and the local society in which it resides or works is the focus of the term on a more local level. Another definition is concerned with the relationship between a corporation and its stakeholders[1].

CSR is an idea, by which the associations coordinate social and natural worries in their business tasks and their cooperation with the partners on a willful promise. An expanding number of specialists and authors have perceived that the exercises of the association have an effect on the outer natural conditions and have proposed that one of the jobs of bookkeeping

should report upon the impact of the association in this regard. There isn't any motivation to feel that investors will endure a measure of corporate non-benefit movement, which considerably causes a decrease either in the profits or the market execution of the stock. Each huge organization ought to be considered as a social undertaking that is a substance, whose presence and choices can be supported as long as they fill public and social needs.

The Principles of CSR

It is difficult to define CSR and to be confident in terms of any such activity because of the uncertainties surrounding its nature. It is consequently critical to be able to detect such behavior. Three major concepts of CSR must be taken into account to include all CSR activities.

Sustainability

The phrase "sustainability" refers to the influence of current actions on future alternatives. If resources are used in the present, they will be useless in the future. This is especially important if the resources are limited in number. As a result, extractive raw resources such as coal, iron, and oil are finite in number and will not be accessible for future use once used. As a result, alternatives will be required in the future to implement the services supplied by these resources. These resources are used in production and manufacturing enterprises. This may occur in the not-too-distant future, but the fact that when resources are reduced, the cost price of the remaining resources tends to rise is a more immediate problem. As a result, businesses' operating costs tend to rise in this manner.

When an organization is viewed as a component of a larger social and economic system, these impacts must be considered not just in terms of calculating the cost and value generated in the present, but also in terms of the future of business. The pace at which resources can be renewed would be included in sustainability measures. Unsustainable operations can be addressed either by developing and implementing sustainable operations or by planning for the future in the absence of resources that are now necessary. In reality, businesses often strive for reduced unsustainability by improving the efficiency with which resources are employed. One energy efficiency initiative is an example. Human resources must be well-versed in the methods and procedures necessary to make the greatest use of resources and ensure their long-term viability.

Accountability

Accountability refers to an organization's recognition that its activities have an impact on the outside world and, as a result, taking responsibility for those impacts. As a result, this idea entails a quantification of the impacts of activities made both within and beyond the organization. More particularly, the notion entails that those quantifications be reported to all parties who are impacted by the acts. This entails reporting to external stakeholders on the impact of activities taken by the organizations and how they affect the functions of the stakeholders. As a result, this idea indicates that the organization is a component of a larger societal network, with duties to the entire network rather than simply the company's owners. Close by this acknowledgment of obligation, there should be an acknowledgment that those outside partners have the power and position to influence the manners by which those activities of the association are taken and the job is played in deciding.

Responsibility requires the advancement of proper proportions of the ecological exhibition and detailing of the activities of the associations. This requires costs concerning the association in creating, recording, and detailing such execution. Benefits should be controlled

by the handiness of the actions chosenfor the dynamic cycles and by the manners by which they work with the distribution of assets. It happens both inside the association and among its different partners. Such revealing must be founded on different attributes. These are comprehension of every interested individual, significance to the clients of the data furnished, dependability as far as the precision of estimation, the portrayal of effect and independence from bias, and equivalence which infers consistency, both over the long haul and between various associations. In any case, such revealing will include subjective realities and decisions just as measurements. This subjective perspective will possess likeness over the long haul and will quite often imply that such effects are surveyed contrastingly by different clients of the data, mirroring their indistinguishable qualities and needs.

Transparency

CSR is a broad topic that generates a wide range of viewpoints and may be approached in a variety of ways. When stakeholders from inside and outside the organization are involved in decision-making processes or developing policies and legislation affecting the organization's goodwill and welfare, they must guarantee that they are communicated to the members. Members will be able to effectively comply with these aspects if they are made known to them. Transparency must also be demonstrated in the execution of duties and operations. The reason for this is that if members of the organization are unclear and confused, they will be unable to carry out their job obligations in a well-organized manner and accomplish the intended results. As a result, it is critical to guarantee that all laws, measures, processes, rules, tasks, and activities are in line with the organization's aims and objectives, with transparency being the most important feature.

As a concept, transparency indicates that the external impact of an organization's actions can be determined from its reporting, and relevant information is not hidden within this reporting. As a result, utilizing the information supplied by the organization's reporting methods, all of the repercussions of the organization's actions, including external impacts, should be obvious to everybody. External consumers of such information, in particular, value transparency since they are uninformed of the underlying facts and knowledge available to internal users of such information. Transparency, then, may be considered as a result of the other two principles, and as a component of the process of recognizing the organization's responsibility for the external affairs of its acts, as well as a part of the process of transferring power to external stakeholders.

CSR Theories

Utilitarian Theory

According to utilitarian theory, the corporation is a component of the economic system that performs a mechanical purpose. It has a long history in profit maximization. CSR concepts develop as a result of the recognition that the economics of responsibility, as well as the corporation's business ethics, are required. The utilitarian theory and the instrumental theories are often used interchangeably. The organization is considered a vehicle for the generation of wealth in these beliefs. Social activities are seen as one of the ways to achieve desirable economic outcomes. Utilitarian theories are also built on the notion of investing in the local community, with the expectation that this investment would provide appropriate resources, amenities, and facilities in the long run, allowing people to enjoy better lives.

Utilitarian ideas are linked to competitive advantage techniques. The proponents of these theories are those who see them as the foundations for formulating plans and tactics for the dynamic usage of a corporation's natural resources for competitive advantages. Altruistic

acts, which are considered social marketing instruments, are also included in the strategy. Altruistic actions are unselfish acts performed for the benefit of the community. According to utilitarian philosophy, a company must recognize social responsibilities and rights to participate in cooperative activities. The functionalist philosophy expressly urges that the company be considered an essential element of the economic system, with profit-making as one of the most important purposes. The organization is considered an investment, and investors and stakeholders want the investment to be productive and lucrative.

CSR was viewed as the industrial system's defense plan against external threats from the standpoint of the internal elements of the firm. The rationale for this is that the economic system's equilibrium should strike a balance between profit-making and societal aims.

Managerial Theory

The administrative hypothesis is worried about the administration of the association. The administrative hypothesis places accentuation upon the corporate administration in which the CSR is drawn nearer by the partnership inside. This is viewed as the central matter of distinction between the utilitarian and administrative viewpoints of CSR. This recommends that every one of the elements that are outside the company are considered. The administrative speculations have been partitioned into three sub-gatherings, these are, corporate social execution, social obligation, inspecting and announcing (SAAR), and social obligation regarding multinationals. CSR for multinationals develops because of worldwide rivalries and difficulties they encountered. This part of the administrative hypothesis appears because of the obligation that the administrators have encountered. This is worked with by characterizing helpful instruments about CSR for the worldwide organizations to get by in outside nations. The individuals from the association needed to settle on moral and shrewd choices, which are focused on the expansion of benefits.

Administrative speculations are likewise emphatically connected with political hypotheses dependent on conceptualization. They put accentuation upon the social obligations of associations that emerge from the power and authority that is vested among people, particularly the ones, who are in administrative roles. The association is perceived as being a resident with specific inclusion locally. The beginning of the political force of CSR depends on Davis's (1960) thought, who suggested that business is the social establishment and it should mindfully utilize power and authority. It is likewise noticed that the causes that create the social power are from inside and outside of the enterprise. Administrative speculations are likewise covered under the integrative hypotheses of Gargia and Mele (2004), to be specific, the elements of public obligation and corporate social execution. Public obligation puts accentuation upon law and public strategy processes that are taken as a source of perspective for social execution. Though, corporate social execution searches as far as friendly authenticity relevant to social issues.

Relational theory

The origins of relational theory may be traced back to complicated firm-environment connections. It suggests that the interrelationships between the two are centered on CSR analysis as a phrase. There are four sub-groups of theories in relational theory. Business and society, stakeholder approach, corporate citizenship, and the social compact are only a few of them. Business and society are defined as "business in society," with CSR arising as a result of contact between two entities. The evolution of economic values in a society is one of the indicators of CSR. Another individual is responsible for taking into account the ramifications of their decisions and actions on the entire social system. Businesses' social duties, expressed

in the form of a general relationship, must reflect their social authority. The stakeholder approach was created as one of the tactics for bettering the organization's management.

The partner approach has been created as one of the methodologies for making enhancements to the administration of the association. It is additionally expressed as the method of understanding reality to deal with the socially mindful conduct of the association. The partner approach further considers an association as the interconnected trap of various interests, where self-creation and local area creation happen autonomously. Corporate citizenship of the social hypothesis firmly relies upon the sort of local area to which it has alluded. It is the methodology that the association needs to embrace to carry out the errands and exercises in a mindful way. Generally, it is about the relationship that an association creates with its partners, and hence, the previous needs to consistently execute the characteristics of responsibility and commitment. At the end of the day, it very well may be expressed that inside the association, the members should frame powerful terms and associations with one another. Thusly, they will want to bring about benefits, efficiency, and occupation fulfillment.[2]

Meaning and Significance of Community Development

When understanding the job of CSR in local area advancement, it is critical to comprehend the significance of the local area. The local area is for the most part characterized as the gathering of people sharing the normal reason. These people need to work as a team with one another for the satisfaction of wanted objectives and destinations. The people group individuals are deferential and circumspect as far as different individuals. There isthe presence of local area pioneers also. The people group pioneers are vested with the power to coordinate and oversee the assignments and exercises. The people group pioneers are the people, who endeavor to impact others to make liability regarding the moves, accomplishments, and local area government assistance.

Community development (CD) is a term used to describe activities done by a community in collaboration with external organizations or enterprises to empower people and groups of persons by providing competencies and abilities. To effect organizational transformation, knowledge, competencies, and abilities are necessary. The knowledge and skills are frequently centered on utilizing local resources and gaining political power via the establishment of big social groupings, as well as participation in duties and activities that promote communal welfare. Individuals working for the community's well-being must be able to collaborate with others as well as influence the community's position within the context of broader social institutions.[3]

The extensively utilized significance of CD is the one given by the United Nations where the CD is viewed as a coordinated exertion of the people locally led in such a way to assist with furnishing answers for the issues with the base assistance and help from the outer associations. One more viewpoint that is connected with CD is about the dynamic inclusion of the people in the issues and concerns, which structure their experience. It is a formative interaction that is both a group and individual experience. It depends on a pledge to rise to support every one of those required to work with the sharing of abilities, information, and experience. It happens both in the areas and networks of interest. At whatever point, people meet up to recognize the significant factors and act as far as the issues of normal concern. Along these lines, it tends to be expressed that the members of the community should recognize the regions inside the local area, which should be enhanced as a customary premise.

Legal Framework of CSR

The Ministry of Corporate Social Responsibility issued Corporate Social Responsibility Voluntary Guidelines in 2009, which was the first formal attempt by the Indian government to bring the CSR problem to the fore. Corporate Relations (MCA, 2009). The relevance of CSR was previously explored in the context of corporate governance reforms, such as the Task Force on Corporate Governance Report, which The Ministry of Corporate Affairs excels (MCA, 2000). It's spelled out in the Voluntary Guidelines.[4]

The main features of a CSR strategy, which included care for everyone, were spelled out in 2009.stakeholders, ethical functioning, employees' rights and welfare, human rights, environmental stewardship, and efforts promoting social and inclusive development

The Guidelines explicitly drew a qualification among generosity of spirit and CSR exercises and featured the deliberate idea of CSR exercises that go past any legal or legitimate commitment. The Guidelines of 2009 were continued in 2011 by the National Voluntary Guidelines of Social, Environmental, and Economic Responsibilities of Business, likewise given by the MCA (MCA, 2011). These rules were allegedly founded on the data sources got from vital partners the nation over and set down nine standards for organizations to work in a capable way to advance comprehensive monetary development at the public level. As on account of the 2009 Guidelines, the 2011 Guidelines were deliberate in scope wherein corporates were asked to take on every one of the nine standards and to report their adherence to the rules dependent on an apply-or-clarify rule. Curiously, while one of the execution techniques recommended in the 2009 Guidelines was to reserve ―a specific sum connected with benefits later expense, cost of arranged CSR exercises, or some other reasonable parameter,□ no such idea was remembered for the 2011 Guidelines. The change from a willful CSR system to a directed system came when the Securities Exchange Board of India (SEBI) required the top recorded 100 organizations, as a feature of Provision 55 of the Listing Agreement, to obligatorily uncover their CSR exercises in the Business Obligation Reports (BR Reports) going with the Annual Reports. This, SEBI believed was in the bigger interest of public revelation and addressed a move towards incorporating social obligation with corporate administration. The most goal-oriented endeavor at ordering CSR exercises for organizations accompanied the institution of Section 135 of the Companies Act 2013 (MCA, 2013). India's new Companies Act 2013 (Companies Act) has presented a few new arrangements which changed the substance of Indian corporate business. One such new arrangement is Corporate Social Responsibility (CSR). Service of Corporate Affairs has as of late told Segment 135 and Schedule VII of the Companies Act just as the arrangements of the Companies (Corporate Social Responsibility Policy) Rules, 2014 (CRS Rules) which has happened from 1 April 2014.

CSR Origin and Development in India

The idea of CSR has been guzzled in Indian culture from the earliest starting point. Gandhi's theory of trusteeship is like CSR of the advanced world; organizations like TATA and BIRLA have been guzzling the situation for social great in their activities for a long time well before CSR become the famous reason. The enthusiastic interest in local area government assistance among the Tata Group dates back to the 1860s when the organization was established by Jamshedji Tata. This clarifies why almost 66% of the value of Tata Sons, the Tata Group's advertiser organization, is held by charitable trusts, which have made a large group of public foundations in science and innovation, clinical examination, social investigations, and the performing expressions.

Dr.Kurien's Amul-drove Operation Flood had spearheaded comprehensive development through work with dairy ranchers at the grass-root level, evolving lives, improving pay, engaging ladies, and at the same time receiving rewards to the business. At Indian Oil, corporate social obligation (CSR) has been the foundation of achievement right from its initiation in the year 1964. The Corporation's goals in this key execution region are revered in its Mission articulation: to assist with advancing the personal satisfaction of the local area and protect natural equilibrium and legacy through a solid climate conscience [5].

Before Corporate Social Responsibility observed a spot in the corporate dictionary, it was at that point finished into the Birla Group's worth frameworks. As soon as the 1940s, the forefather G.D Birla embraced the trusteeship idea of the executives. Just expressed, this involves that the abundance that one creates and holds is to be held as in a trust for our numerous partners. Concerning CSR, this implies contributing piece of our benefits past business, to bring about some benefit for society[6]

Throughout the long term, CSR has acquired significance in India as organizations are understanding the significance of putting resources into CSR for accomplishing advantages of making investor esteem, expanded income base, key marking, functional productivity, better admittance to capital, human and scholarly capital furthermore lower business risk's has arisen as a powerful apparatus that synergizes the endeavors of Corporate and the social area towards practical development and improvement of cultural destinations in general.

The Change in CSR Trends: From Charity to Responsibility

A look back at the history of CSR indicates that it was dominated by the notion of charityuntil the 1990s. Businesses that saw CSR as a philanthropic gesture frequently limited themselves to one-time cash donations and did not devote their resources to such programs. Furthermore, firms seldom considered the stakeholder while developing such programs, lowering the efficacy and efficiency of CSR efforts. The notion of CSR, on the other hand, has evolved in recent years. Giving has shifted from being viewed as a duty or a charitable act to being viewed as a strategy or a responsibility.[7] According to a review of case studies and CSR activity done by Indian corporations, CSR is gradually shifting away from charity and reliance and toward empowerment and cooperation.

Making A Difference CSRInitiatives in Indian Firms

The business sector has only recently begun to see the possibility to assist in the resolution of the issues that CSR addresses. The private sector has come out in support of social responsibility and the government's pledge to give more economic possibilities to the underprivileged.

Policy Initiatives

Understanding the job that can be played by corporate area in tending to a portion of the obvious issues of an emerging country like India, service of corporate undertakings (MCA) is expecting an asset stream of more than Rs 10,000 crore a year from privately owned businesses for social government assistance drives as a component of their CSR later Parliament clears the Companies Bill. When the regulation is approved by Parliament, India would turn into the principal country to command CSR through a legal arrangement. As per the proposition, it will be obligatory for private firms to reserve 2% of their normal net benefit for CSR drives. The public authority needs corporate houses to spend the total in friendly areas, for example, schooling and wellbeing rather than including themselves in individual philanthropy.[8] MCA's draft intentional rules on CSR are along worldwide

standards, for example, morals and straightforwardness, prosperity of representatives, basic liberties, wellbeing and security, utilization of climate cordial unrefined components, following administrative structures, and bigger commitment of partners.

Some Examples of Indian Corporations' CSR Activities

WELSPUN ENERGY LTD is a company that specializes in renewable energy (WEL)Welspun's company philosophy is based on socially responsible and ethical business operations. Welspun Energy has received the ASSOCHAM CSR Excellence Award 2012. Welspun Energy Ltd is a subsidiary of the Welspun Group, a $3.5 billion conglomerate that is one of India's largest.Power generation, infrastructure, and exploration are among the fastest-growing corporations, and oil and natural gas production, as well as steel pipes and textiles

CSR Initiatives

By launching initiatives such as 'Training the Trainer,' 'Enrolling Children in Schools,' and 'Healthy Baby,'Welspun Energy has partnered with local women to create a competition and skill development program for them. Communities to make a good difference in their lives. It is starting to implement social inclusion efforts.

In Madhya Pradesh, Gujarat, and Rajasthan, to demonstrate revolutionary effects. Welspun Energy's leadership is actively active in several forums devoted to environmental issues. The World Bank's Green Growth Action Alliance, the B20's Green Growth Action Alliance, and the World Economic Forum's World Economic Forum's World Economic Forum 'The Steering Committee of the World Economic Forum (WEF).

HUL (RURAL MARKETING)

HUL's CSR philosophy is embedded in its commitment to all stakeholders, including consumers and employees, the environment, and the society the company operates in. The company depends on sustainable sources of raw materials and is committed to minimizing the environmental impact and improving sustainability throughout the value chain.

Gujarat Cooperative Milk Marketing Federation Ltd (GCMMF)

CSR-Orientation to Distributors andRetailers

The GCMMF has recognized distributors and retailers as critical partners in its vendor network. The supplier chain The GCMMF discovered through surveys that 90 percent of distributors do not have access to the most up-to-date management methods. The GCMMF realized it was a mistake. Corporate social responsibility to develop its distributors' fundamental business operations to maintain them in the mainstream of business and compete with those who have formal management training Through Value-Mission-Strategy, the GCMMF has created and educated all of its distributors. Workshops, competency development, Amul Yatra, Amul Quality Circle meetings, computerization, and so forth, and actions involving electronic commerce.

CSR in SMEs

The SMEs in India have developed extraordinarily during the most recent couple of years and have a huge commitment to modern results and products from the country. They represent over 80% of modern endeavors and add to perhaps the most elevated portion of work in the country, particularly in areas like materials, designing, jute, auto subordinate, handiworks and

so on A flourishing SME area is essential as an autonomous and as a supporting industry for enormous ventures just as MNCs.

Mindfulness about CSR is viewed as exceptionally low among SMEs, be that as it may, a considerable lot of them in all actuality do exercises and execute CSR programs without zeroing in on the term 'CSR'[9] The staggering propelling component for SMEs to participate in CSR isn't outer tension however an inner drive to 'making the best choice' or 'returning something' or showing 'enterprising.

SUGGESTIONS

(a) To ensure that CSR is progressively contributing and benefiting, the following suggestions are given to make CSR initiatives more effective.
(b) It is found that there is a need for the creation of awareness about CSR amongst the general public to make CSR initiatives more effective.
(c) Assigning finance regarding CSR as speculation from which returns are normal
(d) Observing CSR exercises and liaising intimately with execution accomplices, for example,
(e) NGOs to guarantee that drives truly convey the ideal results.
(f) A drawn-out viewpoint by associations, which incorporates their obligation to both
(g) inner and outside partners will be basic to the accomplishment of CSR
(h) Organizations follow through on the objectives of their CSR technique [10].

CONCLUSION

Corporate Social Responsibility (CSR) is the idea that has procured greatness in especially business associations. Each company has an arrangement that puts accentuation upon CSR, which delivers a report, yearly, enumerating its exercises. Each partnership can recognize the corporate action, which is publically responsible, and the exercises, which are not publically responsible. The three primary standards of CSR are to be thought about to include all of the CSR exercises, these are, manageability, responsibility, and straightforwardness. The hypotheses of CSR are the utilitarian hypothesis, administrative hypothesis, and social hypothesis. In understanding the idea of CSR, it is imperative to see, how it delivers a huge commitment to advancing successful development and advancement of the networks. Inside the people group, some angles should be thought about, these are changes, prosperity, easing of cultural issues, etc. The people need to utilize information and capabilities to advance prosperity and improvement of the local area.

The jobs of CSR in CD have been recognized in the spaces, which are, to share the unfortunate results because of industrialization, closer linkages between the organizations and networks, assisting with procuring gifts, job in move of innovation, CSR contributes in the insurance of the climate, CSR is for common freedom corporate maintainability, relationship among enterprise and local area, a CSR program is a guide in the lightening of neediness, a CSR program helps in assortment of information, for accomplishment of corporate supportability objectives, advancing social value and advancing sexual orientation balance. CSR has been delivering a critical commitment to promoting prosperity and movement, considering the above-expressed regions. At long last, it tends to be expressed that corporate social obligation is principally worried about the connection betweenthe organization and the neighborhood society. The errands and elements of the company must be placed into activity in such a way that would prompt prosperity and movement of the people and society.

REFERENCES

[1] D. Crowther, *Corporate social responsibility: A broader view of corporate governance*. 2008.

[2] S. Mehedi and D. Jalaludin, "Application of theories in CSR research focusing study context and corporate attributes," *International Journal of Ethics and Systems*. 2020, doi: 10.1108/IJOES-09-2019-0146.

[3] "An International Perspective. The Journal of International Social Research," [Online]. Available: sosyalarastirmalar.com.

[4] Indian Ministry Of Corporate Affairs and W. J. Werner, "Corporate Social Responsiblility Voluntary Guidelines," *J. Heal. Popul. Nutr.*, vol. 27, no. 4, pp. 545–62, 2009, [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/20304693%5Cnhttp://www.mca.gov.in/Ministry/latestnews/CSR_Voluntary_Guidelines_24dec2009.pdf.

[5] "CSR: A Cornerstone of our Enduring Success" Corporate Social Responsibility at India."

[6] "Corporate Social Responsibility Activities by the Aditya Birla Group." http://www.adityabirla.com/social_projects/overview.html.

[7] "Corporate Social Responsibility: Towards a Sustainable Future" , A white paper by KPMG & Associated Chambers of Commerce and Industry of India."

[8] Mahendra Kumar Singh, "Govt sees 10k crore flow from CSR spend," *Times of India*.

[9] Heledd Jenkins, "'Corporate social responsibility–engaging SMEs in the debate', The centre for Business Relationships, Sustainability & Society." http://www.brass.cf.ac.uk/uploads/CSRandSMEs.

[10] Jagg Xaxx, "Recommendations on Corporate Social Responsibility," 2017. https://bizfluent.com/info-8503616-recommendations-corporate-social-responsibility.html.

CHAPTER 3

A STUDY ON INFRINGEMENT OF COPYRIGHT

Dal Chandra, Assistant Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- degautambahjoi@yahoo.co.in

ABSTRACT:

Encroaching copyright isn't new yet existed in different structures in prior many years however today the practice of encroachment of copyright has expanded tremendously practically in the whole globe as well as spreading at a disturbing rate in our nation as well. Presently the opportunity has arrived to secure the freedoms of the creator and to limit the entryway from encroachment with appropriate technique and enactment. The inquiries of encroachment of copyright come into the picture when individuals plan to exploit and make financial misfortune individuals who by the excellence of hard work have acquired those privileges. What is obvious is that the mechanical change has made a generation of copyright material simple and modest, and simultaneously it has made the theft of copyright work straightforward and hard to control.

KEYWORDS:

Copyright, Infringement, Reproduction, Literary, Artistic, Publication.

1. INTRODUCTION.

Man is a social creature. He has a duty toward society to enrich it with his innovative thoughts, works, inventions, and publications. They are public but they are personal property. It is perceived as a characteristic right of a man from the earliest reference point. Be that as it may, continuously, it gained the situation with legitimate rights and came to be known as industrial property. With the progression of time, these freedoms are, presently, known as "intellectual property" and incorporate copyrights. Accordingly, the copyright is a recently arising "legal right identifying with printing, music, correspondence, amusement, and PC and so on. The basic goal of the copyright act is to safeguard the author's interests, as well as the public's general advantages obtained from the author's labors, and to provide remedies for infringement of those rights.

The inquiries of encroachment of copyright come into the picture when individuals expect to exploit and make financial misfortune to individuals who by prudence of hard work have procured those freedoms. What is evident is that the innovative change has made the proliferation of copyright material simple and modest, and simultaneously it has made the theft of copyright work straightforward and hard to control. They have made copyright encroachment global. At the point when a work is communicated from one highlight to another or made accessible for people, in general, to get to, various gatherings are associated with the transmission [1]. These incorporate entities that give Internet access or online administrations. At the point when such specialist organizations partake in communicating or

stamping accessible materials given by another, which encroach copyright or related privileges, they are responsible. Such responsibility could emerge in one of two ways; if the specialist co-op itself is found to have been occupied with unapproved demonstrations of proliferation or correspondence to the public or then again assuming it is considered dependable or adding to or making conceivable the demonstration of encroachment by another. Intellectual property law, today, not just ensure the privileges of the duplicate right proprietor and adjoining freedoms yet additionally manages the subject of public interest and attempts to strike a balance between the two in this computerized climate. Intellectual property law, hence, has covered a venture from its prior days when it used to ensure just abstract and imaginative works, and has entered another world loaded with mechanical advancements [2]. The copyright owner has the sole right to copy his work; ii) issue public copies of the work; iii) rent or lend the work to the public; iv) broadcast of work or incorporate it in a cable program; v) perform, showing, or playing the work in public. Civil and criminal remedies are available for the prevention of the infringement of copyright. In civil remedies, there can be an injunction, and in Criminal remedies, there can be imprisonment and penalties.

2. INFRINGEMENT OF COPYRIGHT

The core of the law of copyright is that it does not let to earn profit and take to himself the work, talent, and capital of another. The law is powerful enough to control what else would be an injustice. At every point in the law of copyright, and of performance rights, the creator of a work has exclusive rightsconcerning specific prohibited activities. If these activities are undertaken by another person, without the authorization of the owner of the copyright, then the individual breaches the copyright in that.

2.1 Section-51 of the Copyright Act, of 1957 defines infringement as

a) Doing something for which no license has been provided by the copyright owner
b) Permitting profit without a license for using a place for the communication of the work to the general public and that communication is infringing of copyright
c) Making for sale or hire, selling or offering for sale or hire distributing, exhibiting in public, or importing into India any infringing copy of the work.

2.2 Elements of Infringement.

Copy, modifying, displaying, reproducing, communicating, or performing a copyrighted work without permission amounts to infringement.

To claim infringement, two elements must be proved:

(a) **Ownership**- the party that has claimed infringement shall prove ownership of the copyright;
(b) **Copyright**- the party must demonstrate that the person who has infringed had access to that work.

1.3 Origin of Infringement in Copyright Law

In India, copyright protection began in 1847, when the East India Company implemented the English Act of 1842 in places that were under its authority. The first statute passed in the year 1914 was the India Copyright Act, of 1974. It remained in existence till after independence, new Copyright Act in the year 1957 was enacted. But then, the Act experienced several

revisions. This act gives protection to original literary, dramatic musical, and artistic works, cinematograph films, and sound recordings.

1.4 Essential ingredients of infringement of copyright

The infringement of copyright happens there is

a) Reproducing work in the material structure;
b) Publishing work;
c) Communicating work to people;
d) Performing that work among the public;
e) Adapting and translating work [3].

The Supreme Court of India in the milestone judgement of **R.G. Anand v. Deluxe Films**, explained the cases in which copyright infringement takes place. The court has set out the accompanying recommendations for holding encroachment of copyright.

(a) There is no encroachment of copyright in duplicating a thought, topic, plot, verifiable or incredible reality.
(b) Where a similar thought is being created alternately, it is obvious that the source isthe same, similarities will undoubtedly happen. In such a case the court ought to decide if the similarities are on a key or considerable part of the method of articulation embraced in the copyright work. If the respondent's work is the exact impersonation of some work that already has copyright, only with some minute changes it might be of encroachment of copyright.
(c) The test is to check whether an onlooker or the viewer after reading or seeing both works has the opinion of unmistakable expression but the resulting work seems, by all accounts, to be a duplicate of the first.
(d) Where there is the same theme but its presentation and treatment are different which makes the subsequent work a new work, no inquiry of infringement of copyright emerges.
(e) If the likenesses show up in two works with material and expansive dissimilarities negativing the expectation to duplicate the first and the occurrence in the two works is simply coincidental, then, at that point, there would be no encroachment of copyright.
(f) As an infringement of copyright adds up to a demonstration of theft, it should be demonstrated by clear and apt proof after applying the different tests set down.
(g) The watcher's test is material to demonstrate encroachment of copyright. Assuming the watcher after seeing the film gets an entire impression that the film is overall a duplicate of the first play, infringement of the copyright might be supposed to be demonstrated. Where, be that as it may, the inquiry is of the infringement of the copyright of a stage play by a movie maker or a Director the assignment of the offended party turns out to be more hard to demonstrate theft. It is shown that dissimilar to a phase play a film has a lot more extensive viewpoint, more extensive field, and a greater foundation where the litigants can by presenting an assortment of occurrences give a shading and appearance not the same as the way where the protected work had communicated the thought. All things considered, assuming that the watcher after seeing the film gets an entirety of the impression that the film is all around a duplicate of the first play, infringement of the copyright might be supposed to be demonstrated [4].

2.5 Criterion for Determining Infringement

(a) There are two central components needed to decide the instances of copyright infringement –
(b) There should be an adequate objective similarity between the encroaching work and the protected work or a considerable part thereof.
(c) The protected work should be a source from which the infringed work has been taken.
(d) The test is to check whether there is a reproduction of the work of the plaintiff in a substantial form. Substantial means the quality of work copied. For example, if the work copied is 10 %, it would not amount to copyright infringement if the core part has not been copied whereas even if 4 % of the part has been copied, it could amount to copyright infringement if the work copied is the cream layer or the most valuable part. So, to find out the substantial part, the court should consider [5].

(a) The worth of the part appropriated;
(b) It's overall worth each work;
(c) The actual reason for each, and
(d) How far the pilfered matter will, due to reproduction of the significant part, will more often than not override the offended party's work
(e) Secondary Infringements of Copyrights

Which Acts Do Not Constitute Infringements - Statutory Exceptions.

The copyright protection given to a proprietor or a licensee is absolute. It is dependent upon exceptions and restrictions. Section 52 of the Act gives an extensive rundown of acts under the heading "certain demonstrations not to, be an encroachment of copyright, which can be called legal exemptions for copyright encroachment. With the end goal of simple understanding, they have been talked about hereunder momentarily, with the assistance of those cases.

3.1 Fair dealing:

The thought of allowing some utilization of a copyrighted work that is viewed as 'reasonable' is normal in numerous wards. For instance, in the USA, intellectual property law has its 'reasonable use' arrangements. In the UK, 'reasonable managing' is permitted corresponding to a copyrighted work. The provisions of fair dealing allow to copy or to use work in an alternate manner which would otherwise be an infringement. It is supposed to be fair dealing if we include 5 percent of others' work in our work for criticism or review. It won't be fair dealing if we include the whole of others' work. Since the amount of work that has been taken may be relevant to the other author but can he ask for the fair dealing provisions to apply to him, this brings us to the question of what is the relationship between fair dealing andthe substantial part of work that has been taken. If the part of the work that has been taken isn't substantial, then there shall be no encroachment of copyright and no compelling reason to depend on the allowed acts. It could be that, at times, the presence of the permitted acts is deceptive. The issue lies in the assurance of the overall edges of generosity and the allowed act in question [6]. In India, under Section 52 of the Copyright Act, of 1957, fair dealing with literature, dramatics, musical or artistry works but is not a computer program, for the following purposes doesn't add up to encroachment of copyright. personal use, including research; analysis, or audit, regardless of whether of that work or some other work.

It could be seen that it is just when the not settled that a significant piece of an abstract, imaginative, sensational, or melodic work, has been taken that any Question of reasonable managing emerges. However, when this Question emerges, the level of generosity, in other words, the Quantity and worth of the matter taken, is a significant component in thinking about whether or not, there has been a "fair dealing" Further while considering if work was fair, it would be done based on whether or not any competition was there between the two works.

A reasonable analysis of the thoughts and occasions depicted in the books or reports would comprise "fair dealing" [7]. Publishing confidential data that was leaked out by some other party does not amount to fair dealing for criticism or review.

3.2 Making of duplicates/ adaptation of computer programs for some purposes:

The creation of duplicates of, or variation of a PC program by the legitimate owner of a duplicate of a such program from such duplicate, to use the PC program for the concurred reason, or for the motivation behind making back-up duplicates absolutely as a transitory assurance against misfortune, obliteration or harm, to use the program for a concurred reason, would not add up to the encroachment of copyright in such PC program. Similarly, the doing of any demonstration vital for acquiring data fundamental for working between operability of an autonomously made PC program, with different projects, if such data isn't promptly accessible, would not add up to encroachment. Further the perception, review, or trial of working of the PC program for deciding the thoughts and standards which underline any components of the program and making of duplicates or transformation of the PC program from a by and by lawfully acquired duplicate for non-business individual use, additionally would not comprise infringement.

1.5 Reporting of current events

Fair dealing of literature, dramatics, music, or artistry works for reporting recent activities, in a newspaper, magazine, or similar periodical, broadcasting or in a cinematograph film or through photography would not establish copyright infringement. However, the publishing of addresses or speeches given out in public isn’t a fair dealing concept of that work under this clause.

1.6 Reproduction in connection with Judicial proceedings

The reproduction of literature, dramatics, music, or artistry works to meet the legal action or for the purposes related to a report of judicial proceedings shall not fall under copyright infringement.

1.7 Reproduction for legislative purposes

The reproduction of literature, dramatics, music, or artistry works in any work that is prepared by the secretariat of Legislatures, especially for using of its members, does not include infringement.

3.6 Reproduction to make certified copies:

Following any law and their supply is not an infringement.

2. SECONDARY INFRINGEMENTS OF COPYRIGHTS

Notwithstanding encroachment of copyright through the demonstrations confined by the copyright in the work, there are sure different encroachments known as auxiliary

encroachments. A portion of the criminal offenses accommodated under the 1988 Act intently follow the comparable auxiliary encroachments and a similar degree of information is needed, for the model, at times know or havethe motivation to accept that the article concerned is an encroaching duplicate. The qualification between essential encroachment and optional encroachment is that the previous includes making the encroaching duplicate or making the encroaching execution, while the last option includes 'managing' those duplicates, giving the premises or mechanical assembly for the exhibition or making an article with the end goal of Making encroaching duplicates. Assuming an optional encroachment has been submitted, there will more likely than not have been a related encroachment of at least one of the demonstrations by copyright.'!' For an auxiliary encroachment, the individual mindful must have information or motivation to accept that the duplicates are encroaching duplicates or whatever [8].

Apparently from the phrasing that the individual included should have either genuine information or, in any event, an emotionally sensible conviction that the important action includes an optional encroachment. Under the Copyright Act 1956, just real information was adequate for comparing optional encroachments, yet all things considered, the courts would in general take a liberal perspective on this and in Columbia Picture Industries v Robinson it was held that, bury alia, the information required stretched out to the "circumstance where a respondent intentionally ceased from request and shut his eyes to the self-evident. The state 'has the motivation to have confidence' in the Copyright, Designs, and Patents Act 1988 Sections 22-26 is new and, in LA Gear Inc v Hi-Tec Sports plc, it was said that it couldn't be understood as per the 1956 Act. The test should be even-handed in that it requires a thought of whether the sensible man, with information on the realities known to the litigant, would have shaped the conviction that the thing was an encroaching duplicate, n the preliminary at the first example, Morritt J proposed that once informed about current realities, the respondent ought to be permitted the adequate opportunity to assess those realities to be in a situation to determine that he is managing encroaching copies [9]. This isn't conflicting with a goal approach - the sensible man additionally may require time for current realities to 'sink in'. Seeking a repayment from a provider after being cautioned that encroaching articles were to be provided demonstrates the presence of 'motivation to accept', Circumstances where it could be conceivable for a respondent not to have 'motivation to accept incorporate where he accepts that the copyright has lapsed, where copyright doesn't remain alive in the work or where the duplicates have been made with the copyright proprietor's permission.

Where official procedures have been started against a litigant charging auxiliary encroachment of copyright, this reality alone doesn't imply that he has the motivation to accept that he is, for instance, making or selling encroaching duplicates. Nor does the way that the litigant had set cash to the side for a battling reserve for the forthcoming prosecution show that he has the essential information: Metix (UK) Ltd v GH Maughan (Plastics) Ltd. After all, the respondent might consider that he has a decent possibility of effectively protecting the activity since he doesn't feel that the duplicates are encroaching duplicates or that he didn't have the motivation to accept that he was encroaching at the applicable time. The need to show a psychological component concerning an auxiliary infringer should be stood out from the demonstrations limited by copyright under areas 16-21, in which the question of the infringer's psychological component doesn't emerge, if he submits one of the demonstrations, he encroaches on copyright whether or not he realizes that copyright stays alive in the existing work and whether or not or not it is sensible for the infringer to think that copyright stays alive in the work. The severity of this situation is tempered by the way that the accessibility of the cure of harm is subject to the infringer's psychological state.

3. LAY OBSERVER TEST

By and large, the Courts in India follow the 'lay observer test' to decide encroachment of copyright. As indicated by this test, "whether or not there has been an infringement of copyright is to check whether the pursuer, onlooker or the watcher in the wake of having perused or seen both the works ought to be obviously of the assessment and get an indisputable impression that the ensuing work has all the earmarks of being a duplicate of the first. On the off chance that to the "lay observer," it would not have all the earmarks of being multiplication, there is no encroachment of copyright underway. Before this view was maintained by the Kerala High Court in R. Madhavan versus S.K. Nayar, which held that divergent books don't include encroachment of copyright. The Delhi High Court set out that the encroachment of copyright must be tried on the visual appearance of the drawing and the item in Question. The motivation behind useful utility, adequacy of various parts, and parts of the article or the material of which they are made is important with the end goal of copyright. The expansion of law books from understudy versions to legal counselors' releases doesn't add up to the encroachment of copyright. Comparably play, dramatization, or film is created dependent on the genuine life occurrences detailed in Newspapers, however,uniquely doesn't prompt the encroachment of copyright. Distributing notes from the schedule endorsed by the college isn't encroachment of copyright On the other hand, making the reproduction of a unique picture. Colorable restriction of work and unapproved broadcasting to the overall population add up to the encroachment of copyright. Indeed, even a promotion by an individual asserting a direct copyright that was claimed by another and proposing to sell the equivalent establishes an encroachment of the right.

SPECIAL PROVISIONS CONCERNING SOUND RECORDINGS AND VIDEO-FILMS

The Amendment of 1984 of the Copyright Act, embedded another provision Section 52-A, following the recording of sound and video films. This arrangement manages the points to be inserted in Sound Recordings and Video Films. The objective behind such an arrangement is that it looks like it is of the fragile nature of the copyright in video films and audiocassettes. Now, the consequence of this provision is that no one shall be publishing a sound recording about any work unless the following things are given-

the names and addresses of the persons who make the sound recordings; the names and addresses of the owners of the copyright in such works; and the year when it was first published; likewise, no person is allowed to publish a video film regarding anything until the below-mentioned provisions are displayed in that video film, when shown on the video-holder or other container thereof, viz:- assuming that such work is a film, guaranteed for presentation under the arrangements of the cinematograph Act, 1952, an authentication conceded by the Board of Film certificate; the name and address of the maker of the video film and the subtleties of the import permit and assent; and the name and address of the proprietor of the copyright in such work; These points of interest remembered for sound accounts and video films help the avoidance of video-robbery and theft and sound tapes [10].

4. CONCLUSION

Copyright infringement occurs when someone other than the copyright holder copies the "expression" of a work. This means that the ideas or information behind that work is not given protection, but how the ideas are expressed is given protection. For example, there may have been some movies related to Pirates, but Jack Sparrow is only one. Copyright infringement occurs even if somebody is not copying a work the same same. The given

example of copyright infringement perfectly fits the case of music and art. Copyright infringement occurs if the work infringed is "substantially similar" to the work that is given copyright protection. The copyright owner has many rights and these rights can either be sold or assigned. The right is to reproduce the work meaning any copy can be made in a particular period and apart from the owner of that copyright, if someone else uses that copyright then it is a copyright infringement. The second right is to produce derivative work meaning modifying the original work and creating new modified copies from the existing work. Another right with copyright holders is that of distribution meaning the owner can bring his work to the public utilizing selling, renting, etc.

REFERENCES

[1] R. Watt, “An Empirical Analysis of the Economics of Copyright□: How Valid Are the Results of Studies in Developed Countries for Developing Countries□?,” *Econ. Intellect. Prop.*, 2009.

[2] J. Saraswat and R. Chaturvedi, “Copyright protection in the digital environment: Indian perspective and international obligations,” *J. Intellect. Prop. Rights*, 2017.

[3] K. Kariyawasam, “Artificial intelligence and challenges for copyright law,” *Int. J. Law Inf. Technol.*, 2021, doi: 10.1093/ijlit/eaaa023.

[4] S. Singh and Aprajita, “Insight into the nature of the offence of copyright infringement,” *J. Intellect. Prop. Rights*, 2008.

[5] A. Krishnan, “Testing for Copyright Protection and Infringement in Non-Literal,” *J. Intellect. Prop. Rights*, 2005.

[6] A. Sharma, “Indian perspective of fair dealing under copyright law: Lex lata or lex ferenda?,” *J. Intellect. Prop. Rights*, 2009.

[7] S. Nugroho, D. Praptirahayu, and M. Y. A. R. Sari, “Fairness in Fair Dealing on the Industrial Design Protection,” *Yuridika*, 2021, doi: 10.20473/ydk.v36i2.26009.

[8] C. Oppenheim, “A copyright overview,” *Prof. la Inf.*, 2020, doi: 10.3145/epi.2020.ene.06.

[9] H. R. Jamali, “Copyright compliance and infringement in ResearchGate full-text journal articles,” *Scientometrics*, 2017, doi: 10.1007/s11192-017-2291-4.

[10] “Copyright for Sound Recordings,” *Am. J. Comp. Law*, 1972, doi: 10.2307/839318.

CHAPTER 4

COMPULSORY LICENSING OF PATENTS IN INDIA

Bishnanand Dubey, Assistant Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- bishu.dubey@gmail.com

ABSTRACT:

A patent is described by the WIPO itself as a right that is granted for an innovation, which may either be a product or a technique, which provides a new way of accomplishing a given thing or which gives an inventive technological solution to any existing issue. The patentee obtains exclusive rights to the innovation which has already been patented for twenty years. He also can stop other individuals from utilizing his patented goods. However, there are instances whereby a third party may be entitled to make fair use of patented goods. The Indian Patent Act, 1970 underneath Chapter XVI explores this notion. Compulsory licenses may be described to be licenses that are issued to any person or a firm that desires to utilize the patent or other intellectual property by the authorities. The owner's permission under such situations is irrelevant. Developing nations have put a lot of significance on the supply of obligatory licensing partly because the medications in such countries are seldom accessible and even when accessible are not cheap for the public. However, industrialized nations such as USA or Countries in Europe are resisting the award of obligatory licenses since it reduces the scope of the invention. In this investigation, the Author has concisely addressed the idea and genesis of the concept of compulsory licensing before going towards its status and acceptability at the worldwide level. Further, the Author has put attention to the requirements which are embedded in the Indian Patents Act, of 1970. Moreover, the Author also treated briefly the ramifications of the award of obligatory licensing both at the domestic and the international level.

KEYWORDS:

Patents, World Intellectual Property Organization, Inventions, Compulsory Licensing, Innovation.

1. INTRODUCTION

The Patents Act, of 1970 has been amended thrice and in the year 2005, it included 'compulsory license' under sec 84-92 of the Indian Patents Act, 1970. A patent grants an exclusive right to prohibit or restrict others from commercially utilizing the protected innovation. In other terms, patent protection implies that the innovation cannot be commercially manufactured, utilized, disseminated, imported, or sold by anyone without the patent owner's approval. In India, this right is bestowed by the law and it is for a term of twenty years from the date of publishing. However, this provision of the exclusive right of using a patent is indeed not comprehensive and in some cases, other parties might be authorized to utilize a patent by the issue of a Compulsory license. They may also be described as the forced agreements between two parties when the seller is hesitant to sell however the buyer is eager to purchase and the State has compelled or coerced the seller to

trade. The owner is paid a price that is determined in exchange for the license by the person or the firm who has been given the obligatory license.

Compulsory licensing is when a state authorizes a third party to make a patent product or process without the approval of a patent owner or intends to utilize the patent-protected innovation itself. Compulsory licensing is regarded to be the backbone of the present patent laws. Accessibility of people to inexpensive, quality, generic medications is undoubtedly the cornerstone for making therapies that may prolong life widely accessible to all those who need them. It may also cut the pricing of the pharmaceuticals if they are scarce or unaffordable. It further also permits generic competition and permission to create or sell to rivals after cutting the pricing. The most notable alternative for tackling the challenges connected with procurement, boosting local availability of pharmaceuticals, and cost-efficient for the patient and the government's budget health is the award of obligatory licenses for manufacturing generic drugs domestically. Generic competitiveness as well as the permission to sell or manufacture to any rival at a lower price is permitted under the licensing system. For perhaps the first instance the TRIPS Agreement gave birth to such variables which may put pharmaceuticals that were formerly out of the grasp of ordinary people also within their grasp in the developing nations. This matter was also debated to a considerable degree at the Doha Ministerial Conference held in Nov 2001, wherein it was clearly stated that member nations have been granted enough flexibility and freedom to determine the ground for giving compulsory licenses. Additionally, they have the authority to make changes in the legislation [1].

2. DISCUSSION

2.1. Compulsory Licensing Under International Law

2.1.1. Paris Convention

The formation of a framework allowing the inventors to be able to safeguard their innovations at the worldwide level was the only goal of the Paris Convention. Article 5 provides that “Every contracting state should have the authority to adopt legislative measures, allowing for the issue of obligatory licenses to avoid the outcome of the exercising the exclusive rights given by the patents, for instance, refusal to work”.

2.1.2. TRIPS Agreement

Article 31 of the TRIPS Agreement allows the right to use a protected product without the authorization of the patent owner subject. However, this was restricted to specific conditions:

(a) Permission to make appropriate use of patented goods should be considered exclusively on individual merits;
(b) Such use might be approved only if, before any use of it, the user proposing such a proposal has made attempts on a personal basis to acquire consent from the proprietor of the patent on these commercial terms and circumstances which are fair. However, such initiatives have not shown any success within the appropriate length of time. But, it must be emphasized here that this condition may also be set off by any participant in scenarios that calls for a national crisis or such other conditions which are of great urgency or in instances that include non-commercial usage;
(c) The period and the scope of use of the patented product must be restricted solely until the accomplishment of the objective for which it was granted;
(d) Such usage shall not be exclusive;
(e) Such usage shall not be assignable;

(f) Any such use must be approved principally for the exclusive purpose of supplying the home markets of the member allowing such user.

2.1.3. Doha Ministerial Declaration

It was adopted on 14th December 2001. Access of everyone to medications has long been a controversial topic. It was finally concluded at the Doha Round of Talks of the Development Agenda (Doha Development) by the WTO. The primary themes which were stressed in the Doha Development were:

(a) Interpretation as well as execution of the TRIPs Agreement in such a way that is also supportive of public health. This needs to be done by supporting both simple access to those pharmaceuticals which are in existence as well as to research and development for the manufacturing of new drugs.
(b) The TRIPS Council must be offered advice set up by the principles as well as the goals contained under Articles 7 and 8 of the TRIPS Agreement. It must take into consideration totally the development dimension.

2.1.4. Separate Doha Declaration on Public Health

It was approved on 14 Dec 2001. The magnitude of challenges linked with public health which was impacting growing as well as underdeveloped nations was acknowledged. Special focus was paid to illnesses such as HIV/AIDS, TB, malaria, and some others. The necessity of protecting intellectual assets was acknowledged for the development of medications. The biggest issue was the consequences it had on the procedure. It was acknowledged by all that the TRIPS Agreement ought not to be restricting the members from undertaking any such actions which in their judgment are vital for the welfare of the majority and was also recognized that the TRIPS Agreement does not do. It was ruled that the Deal must be understood as well as executed to preserve public health and facilitate the availability of pharmaceuticals to everyone. This was entrusted to the members to select the basis over which compulsory licenses would've been given in their region. Each participant was assigned the discretion to determine what might comprise a national emergency for them. Each member was granted the flexibility to construct the regime for fatigue, but, it was subjected to the MFN and the National Treatment policy. The member nations of WTO that have restricted access tothe manufacture of pharmaceutical medicines should make good use of the policy of compulsory licensing. Therefore, the Doha Decision provided the nation's freedom to obtain pharmaceuticals. The nations with low or no manufacturing capacity must provide obligatory licenses to any existing patent. The nation that has the potential to produce must do so instead of other countries and should provide it in an atmosphere that is safeguarded.

On 6th Dec 2005, the amendments in the TRIPS Agreement were adopted by the WTO member nations. A permanent ruling was taken on the question of patent and public health which permitted the countries that have insufficient manufacturing capabilities to import medications that are manufactured under compulsory licenses in other states. Article 31 of the TRIPS Agreement permits a member country to establish legislation that may authorize a third party to create a medication that has previously been patented without any approval of the proprietor of the patent in instances of national emergency, extraordinary urgency, or non-commercial public usage. Thus, compulsory licensing is the globally acknowledged legal procedure thatis employed to remove the restrictions on access to inexpensive pharmaceuticals. Article 31 further offers the right to issue of coercive license once the attempts in the negotiation of a voluntary license do not see any progress in a reasonable time

frame. Therefore, it can be claimed that there are unlimited alternatives to organize the award of obligatory licenses which has evolved from the TRIPS Agreement and the Paris Convention and has been defined in the Doha Declaration on Public Health.

2.2 Compulsory Licensing in India

The Indian Government holds the authority for awarding forced licensing. It may be given for any form of being used of all those special rights that are provided to a person by the patent in cases such as national crisis, extraordinary immediacy, or non-commercial usage by the public. The non-commercial usage by the public includes the crises contributing to public health difficulties resulting in illnesses such as AIDS, TB, cancer, malaria, etc. Compulsory licensing is a key topic that demands a full investigation, with special emphasis on Sec 84, 92, and 92A of the Indian Patent Act. Moreover, according to sec 117- A, an appeal may be made even for obligatory licenses. It should be highlighted here that when issuing the obligatory license, the Controller has had to consider the invention's nature, the period which has gone, the capacity of the applicants, and their efforts in securing the license on acceptable conditions. While giving a compulsory license to a 3rd party, an appropriate royalty is given to the patentee concerning his kind of innovation, the usefulness it provides, and the expenditures which has been expended in maintaining the patent grant in India, among other variables. In typical instances, the request for the award of compulsory license is first publicized and the patent holder as well as other interested people are given appropriate time and chance to defend the transfer of patent to the 3rd party. However, in instances such as those of national emergency, or other exigent conditions, where it becomes essential to take quick steps in the interest of the public, the Controller may first award the license and then inform the patentee and other concerned parties to make any objections. Under certain specific situations such as those of medical crises which are backed by the existence of the notice by any foreign nation in that respect, the Controller might have to meet the medical crisis in that nation and award compulsory authorization [2].

2.2.1. Grounds of Compulsory Licenses: Sections 84 and 92

To encourage the inventors to display their discoveries and provide monopoly rights to the patentee to exploit their creation and prevent everyone else from performing any unlawful use of the innovation, patents are awarded. The key purpose behind the award of patent rights in India is assuring the works of innovations in India on a commercial scale and also to the level without any excessive delay. The central government, if convinced that the obligatory license is essential to be provided in the interest of the public, it may be granted at any moment. Any individual who is concerned about making use of a patented innovation for public welfare may make an application before the Controller for the issuance of an obligatory license after the expiration of 3 years after a patent has been granted. This is nonetheless susceptible to certain grounds:

1. For easing the transfer of technologies
2. For enhancing public nutritional status
3. For fostering socio-economic growth, commerce, etc
4. For enabling legitimate requests of the public that did not meet relating to the patented innovation
5. The innovation is not provided to the public at affordable pricing
6. The innovation is not being utilized in the Indian territory
7. A case of national crisis
8. A circumstance of extraordinary urgency
9. A scenario of non-commercial usage by the public.

2.2.2. Reason for Granting Compulsory License: Section 89

In the majority of the circumstances, the required license emerges as an expedient answer to the concerns of procurement. It assists in boosting the supply of pharmaceuticals locally and also reduces expenditures towards the national health budget and sufferers. It also enables the Ministry of Health to enhance its authority in the acquisition of pharmaceuticals from providers that are not dependent on the patentee. It also enhances the availability of medications at cheap costs for patient populations and other developing nations. It also enhances generic competition and subsequently offers the rivals the authorization to develop or sell pharmaceuticals at reduced rates. Objectives of the required license are: 1. The innovations that are patented should be used and worked inside the Indian territory commercially. Any individual that has an intention of working or advancement of an innovation within the territory of India is not unfairly or adversely affected under the safety of the patent; 3. The patented innovations are made publicly available at negligible prices [3].

2.2.3. An Application of Compulsory License: Section 84(6) and 92

The application that is submitted for obligatory licensing comprises a declaration that sets the kind of interests of the applicant including other specifics which may be mandated and also the circumstances upon which the application is built. Whereas if Controller has contended that no satisfactory necessities of the general populace have been fulfilled by the patented discovery or no work is managed to carry out in the territory of India with the patented innovation or that the innovation is unavailable at a fair price to the people, then he may give compulsory license, on contexts and something that he thinks match up. On having received an application by an individual for a compulsory license, the Controller considers factors such as innovation nature, the time that elapses since the patent was granted to the patentee, and the measures taken by the patentee or other individual interested in the patented innovation in complete usage of invention, the potential of the claimant to improve the use of the innovation to the public benefit, the skill of the claimant to undergo the threat involved in delivering capital and also working the discovery, if the application has been granted, the attempts put by the claimant for obtaining the permit from the patentee on terms of service which are reasonable and further proof that the efforts did not yield any successful result within a reasonable time frame. The obligatory license may be given at any time following the award of a patent. It is proclaimed through a notice in the Official Gazette.

2.2.4. Process to deal with Application of Compulsory License: Sections 87, 88, 91

Where the Controller is pleased with the request, he must give instructions to the applicant to give those copies of the application first to the patent owner and to any other person who, as per the records, is engaged in the patent in regards wherein the application is filed by the claimant and that application would then be posted in the official journal. The patentee or any other individual who intends to raise a protest against the issue of obligatory license to the claimant may send such notification to the Controller of his disagreement. Such notification must include a statement which outlines the basis on which the request has been challenged. On receiving such validly served, the Controller shall inform the applicant and must provide both sides the chance hearing before issuing the judgment. An individual who would have the authority to make better use of the other patented product, or who is a patentee or a licensee, could reach Controller for granting a license of the patent described on the reason that he is been obstructed or precluded from using the patented product to its benefit or proficiency.

Where the controller is pleased, an order might be issued by him on conditions that he believes suitable for granting a license under the first specified invention and also a

corresponding order for the second patent, if it is asked. The license is provided with the exclusive aim of delivery of the patented goods in the Market in India and in certain circumstances, also for exporting. If the application is filed by the holder of a license, the Controller could also decide the termination of the current license on granting of a new license or might even make the order for adjustment of the present license. If an individual is an owner of many more patents and where the Controller is pleased that it wouldn't be feasible for the claimant to perform under the license given to him for a patent without overstepping the other, by which both the patents engage technical advancements or huge economic importance, he may command the approval of license in regard of all other patents also to empower the license holder to make better use of either the patents. Whenever the requirements and criteria of the license are determined by the Controller, the licensee might make an application to the Controller for changing the criteria and requirements after the expiration of 12 months [4].

2.2.5. Refusing to Grant a License: Section 84(7) (7)

A patentee may decline the issuance of a license on some reasonable criteria which are expressly indicated in Sec 84(7) of the Patents Act, 1970. The causes are:

1. There may be a commerce or industry functioning or any growth or creation of new sector or commerce in India or trade or industries of any individual or class of people who are dealing or producing in India is affected;
2. The claimed invention isn't in demand on acceptable terms or at a sufficient scale;
3. No supply or growth of the sector for exporting patented innovations that are made in India is there;
4. The creation of the installation of the patented innovations which are made in India is biased;
5. If manufacturing, sales, or use of substances are not covered by the patent, due to the obvious requirements which are placed on the patentee regarding issuance of licenses underneath the patent;
6. Where a condition is put on the patentee about the grant of license to give the grant back;
7. If the idea is not being developed upon a commercial basis inside the Territory of India
8. Where there are restrictions in operating patented innovation for commercial applications inside India [5].

2.2.6. Adjourning Applications for Compulsory Licenses: Sec 86

Whenever an application for granting a compulsory license is submitted upon the ground that no work is being done on the invention or that the patentee has declined to give the license, so after the contentment of the Controller that sufficient time has passed since the patent has been granted and no enough work is done on a commercial level that involves the patented product, and for allowing the invention to work on a commercial level to its maximum capacity which is sensibly feasible, he can command adjournment of any other hearing for a period he thinks fit for working of the invention but it shall not exceed 12 months. But, no postponement may be allowed until the Controller is pleased that the patentee has taken all the appropriate or reasonable measures for the functioning of the product on a commercial level inside the Indian land.

2.2.7. Requirements and Restrictions for Compulsory Licenses; Section 90

The Controller shall strive to acquire the terms and circumstances of the required license. They are:

1. Any payment, including royalty, shall be reserved for the patent holder or other person who is legitimately eligible for such privileges;
2. The patented idea is being exploited to its utmost extent by the individual who has been awarded the license plus he is also rewarded with fair profits;
3. The patented innovation is made accessible to the general public at affordable pricing;
4. The licensee is given exclusive privileges;
5. The privilege given to the licensee cannot be transferred by him to another individual
6. The license is issued for a time and is applicable only until a shorter period following the interest of the public is available;
7. The primary goal of issuance of a license is the distribution of the innovation in the Market in India or the shipment of patented goods to a specific amount;
8. The license is provided for the functioning of the innovation for non-commercial community use if it is anything linked to a semi-conductor technique;

The license holder must not be entitled to ship the patented invention if such import would violate the rights of the patentee. However, the Central Government may instruct the Controller to permit a licensee to bring a patented innovation from overseas, if according to him it is required for larger community welfare, and the Controller shall give effect to these directives [6].

2.2.8. Compulsory License for Pharma: Sec 92A

The compulsory license is indeed available for manufacturers and exporting pharma that is patented to any nation that cannot address health care issues about pharmaceutical areas, only if the nation has particularly given the compulsory license., The controller on receipt of the application in the procedure provided, gives the license specifically for manufacturing and exporting the given item to the nation under provisions posted by him [7].

2.2.9. Cancellation of Compulsory License; Sec 94

When a patentee or some other individual who has an interest in the patented product applies, the compulsory license given might be revoked by the Controller, when according to him the situation due to which the compulsory license was granted does not exist now and that situation will not occur again.

2.3. Consequences After Granting Compulsory Licensing

The granting of obligatory licensing comes with its own set of drawbacks. On one side it gives an advantage to the general population as it shields a great part of their health difficulties by making the delivery of life-saving pharmaceuticals at a reduced cost, but the long-term advantages are not that simple to be realized. There has to be a suitable proportion between the States who is the authorizer, the license holder who are people at large or the private enterprise engaged in the manufacturing and production of generic medications, and the owner of the copyrighted innovation who may be the reluctant patent holder. The award of an obligatory license discourages the patentee from participating in any creative activity in the long term. It also generates a grey economy due to demand in huge numbers in local

marketplaces. The Biotech Industrial Corporation has assumed that the award of a compulsory license helps in generating drug at a cheap cost and also safeguard healthcare, mostly in India since there is a lack of certainty regarding nobility or interest that likewise minimizes the scope of discovery. The makers that create generic medications are likewise prohibited to export the product, particularly if the supply is entirely for the local market. Moreover, the notion that payment of a suitable quantity of fee is connected with the issue of required licensing may enhance the cost of the pharmaceuticals. Therefore, the issue of compulsory licensing is not the final option for making the pharmaceuticals available to people since it might lead to lower projects in India as the innovators would search for a more corporate-friendly legal framework. Additionally, the royalties provided are indeed not even near to the economic advantages that the patent holder obtains if he applies his exclusive right to his innovation, instead, the licensee obtains the benefits without actually participating in the research and advancement of the innovation. There is also a concern concerningthe provision o substandard pharmaceuticals to customers since there is a lack of authority to monitor the manufacturing and production of generic medicines. Nevertheless, by having taken a literature review as to the repercussions of compulsory license on the investigation and advancement of the evolving drugs that are patented, it could be said that licensing agreement eliminates the desire to keep innovating and it has a huge effect on the pharma companies that are carrying on it the obligation to meet the healthcare problems of such a huge Indian population. The procedure that is involved in the creation of pharmaceuticals is quite expensive and dangerous which makes the patent system of drugs far more vital. This impacts the pharmaceutical business to suffer to a significant degree since the issue of forced license diminishes patent protection and jeopardizes investments and also advancements. Hence, there is difficulty in front of the decision-makers to guarantee that the schemes that might undermine the invention but at the given time can increase the accessibility of the public towards the pharmaceuticals so that the least damage is given to the research and investment sector. The places which will be touched by obligatory licensing are as follows: -

3. *Innovation:* In the developing world, the creation of pharmaceutical businesses will be reduced since they will be relying on generic pharmaceuticals. They would prefer having the obligatory license to a generic medicine rather than investing the Exploration & Development independently, which is frequently a very expensive item. Additionally, inquiry-based pharmaceutical corporations would not initiate patent modules in underdeveloped nations since there's always the danger of loss of patents and loss of capital in research.
4. *Competing and Cost:* Compulsory licensing would boost the number of firms providing generic pharmaceuticals. Thus the aggregate supply would increase, and the price would drop. This would also compel the innovative nations to provide different prices of respective patent modules ensuring that they could survive in the market.
5. *Patients:* Service users will acquire drugs at a much lower cost. Furthermore, large pharmaceutical firms typically create proposals like free access to medication to safeguard their patent in developing nations. Compulsory licensing seems to have established the hope for financially constrained patients in undeveloped nations. India requires this service because of the economic status of the majority of people. But the difficulty is that on one side, it needs to adhere to international norms of patents while on the other, it has to ensure public health [8].

6. CONCLUSION

The concept of forced licensing should be utilized wisely since it is an exceptional case and a flexible case to the general norm of the patent. The clause comes mid-way; neither complete patent protection is provided, nor is it refused because it directly impacts innovation

financing and uncontrolled application of this clause may result in international pharmaceutical corporations being cautious to propose novel medications in other nations. Hence the corporations have to establish the pricing of their patented module according to the economic situation of the nation if they want to safeguard their item from forced licensing. Compulsory licensing has recently emerged as a hope for credit-constrained patients in undeveloped nations. India requires this service because of the economic status of the majority of people. But the difficulty is that on one side, it needs to comply with various norms of patent protection while on the other, it will have to ensure public health [9].

Safeguarding a patent, albeit not entirely clad, yet remains functional while giving a drive towards the innovation and development of new items. If we have a glance at the pharma patent, then it could be mentioned that they could only operate successfully in developed nations where the buying power of the members of the society is significant which makes it simpler for them to have access to medications. Compulsory licensing consequently, has to establish itself to be a lifesaver for the emerging nations too. It is not questioned that the national court of India does exhibit its potential in redefining the diplomacy linked to public health and also impose such standards by holding the pharmaceutical corporations liable for their commitments in the business sector regarding access to medications. Though the privileges of the patent owners become prejudiced with rulings like these, a holistic perspective also demonstrates that these judgments do assist in affirming the rights of the citizens to access pharmaceuticals which is one of the most critical parts of health and consequently to the Right to Life. But, simultaneously, that is only in its confined and well-explained use together with all the required safeguards that can only maintain the right balance between invention, investment, and competitiveness. The correct and effective usage system of the issue of obligatory licenses like a weapon in the legal domain would undoubtedly benefit India in the development of the transfer of technology. Hence, India should avoid weakening and also underutilizing the mechanism of compulsory licensing only for the sake of exporting or for expanding the economy of scale. Furthermore, where the trend of compulsory license ramps up and is being managed adequately, it would further lure a lot of investments, which would eventually lead to an overall rise of Foreign Direct Investment, and thus placing India up in the queue of the economic development [10].

REFERENCES

[1] R. Chaudhry, “Compulsory licensing of patents in India,” *Pharm. Pat. Anal.*, 2016, doi: 10.4155/ppa-2016-0033.

[2] H. Chander, V. Choudhary, and V. Kumar, “Current scenario of patent act: Compulsory licensing,” *Indian J. Pharm. Educ. Res.*, 2013, doi: 10.5530/ijper.47.3.5.

[3] S. Basheer and M. Kochupillai, “The ‘Compulsory Licence’ Regime in India: Past, Present and Future,” *SSRN Electron. J.*, 2012, doi: 10.2139/ssrn.1685129.

[4] S. Vig and T. Bagga, “Compulsory licensing of patents in India,” in *Patent Law and Intellectual Property in the Medical Field*, 2017.

[5] K. D. Raju, “Compulsory v voluntary licensing: A legitimate way to enhance access to essential medicines in developing countries,” *J. Intellect. Prop. Rights*, 2017.

[6] V. V. A. Le, “Compulsory Licensing of Patented Pharmaceuticals in the Developing World: A Legitimate or Illegitimate Way to Enhance the Access to Medicines?,” 2018.

[7] P. K. Saha and A. Mukherjee, “Compulsory licensing of pharmaceutical patents in India a policy shift,” *Economic and Political Weekly*. 2019.

[8] V. Prasad and P. S. S. K. Babu, "Compulsory licensing: Implications on multinational drug companies," *Int. J. Intellect. Prop. Manag.*, 2013, doi: 10.1504/IJIPM.2013.057621.

[9] R. K. Sehgal and R. L. Koul, "Whither to public interest-the curious case of compulsory drug licensing in indian pharmaceutical industry," *Indian J. Forensic Med. Toxicol.*, 2020, doi: 10.37506/ijfmt.v14i4.13202.

[10] V. R. K., G. K., and H. R., "Compulsory licensing - The effect on generics, patents and drug-development in indian pharma industry," *Indian Journal of Pharmacology*. 2013.

CHAPTER 5

COPYRIGHT PROTECTION FOR DATABASES IN UK AND INDIA

Praveen Kumar Mall, Associate Professor
College of Law, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- drpraveenmall@gmail.com

ABSTRACT:

Databases are often thought of as static warehouses where vital data and information are stored. With the rise of e-commerce, whole companies are being built around databases, with income streams coming from membership fees, royalties, and advertising. Database producers secure their compilation efforts to recoup their original investment of time, money, and expertise, as well as to discourage parasitic competition. As a result, a corporation is effectively discouraged from participating in the information age if it cannot control access to and use of the databases it produces. Although databases have generally been protected by copyright rules, improvements in information technology have allowed rivals and pirates to engage in market-destructive copying. Furthermore, after the Feist judgment, the needed degree of originality in many countries has been in flux in recent years, notably in the United States and Europe. The status of databases in India is guided by the philosophy of rewarding labor, time, and money investment with a minimal necessity for originality. A few criteria have been proposed that might be used to draft new legislation that balances private and public interests while keeping the core goal of the intellectual property regime in mind: to stimulate creativity and innovation while maintaining a vibrant public domain.

KEYWORDS:

Database, Copyright Protection, Originality, Sui Generis, European Union.

1. INTRODUCTION

A database can be defined as an aggregate of data that is organized for easy access, management, and update. It is a collection of information arranged and fixed and systematically stored in any form of media. The database is created to spread information from various sectors such as agriculture, health, science, environment, etc. Copyright protects the expression of information and not just the idea. Formalities such as registration are not required to protect a work under copyright. Copyright aims to protect the creativity of the creator. Doctrines like arbitrary competition and misappropriation have been used by many courts to safeguard database manufacturers from losing their work to people who just republish the work of the original manufacturer who used sweat of the brow to make it. Databases are collections of data that allow for the selection and organization of data based on characteristics defined in the database. Raw data, which is a source of knowledge or entertainment value, and tools, which are programs that may be used to transmit, store, or alter raw data, are the two types of digital property found in a database, or information system. A fully formed database is a collection of interconnected components capable of extracting value from data collection, processing, merging, storage, and distribution [1].

A complicated array of potentially protectable intellectual property is included by the several entities grouped under the title of 'database.' The data items themselves, as well as the work used in discovering them, any creativity involved in picking and organizing the accessible pieces, and the search and organization tools, as well as all parts of their production, are the main categories.

Databases have traditionally been considered literary works, with copyright protection in many nations. Database creators confront a unique issue in protecting the data they have compiled: facts cannot be copyrighted, but an arrangement of facts, such as a database, may be copyrighted if it 'includes an original selection or arrangement' that 'possesses at least some basic degree of inventiveness.' Database rights are rights granted in exchange for labor and investment, rather than for invention or innovation. Because creating a database is a costly and time-consuming process, the most compelling reason in favor of database security is the prohibition of competitor copying. The individual who copies, on the other hand, is not responsible for the original compiler's development expenditures and so can undercut its price.

The Berne Convention Article 2(5) contains an international reference to the legal protection of databases, which states that "a database is a collection of literary and artistic work, such as encyclopedias and anthologies, which, because of the selection and arrangement of their contents, constitute intellectual creations." TRIPS loosens the Berne Convention requirement by permitting protection based only on originality in the selection of works to be assembled or in the arrangement, and by expanding the concept of compilation to encompass data and other information in any form. The most current WIPO Copyright Treaty of 1996, which went into effect in 2002, defines data compilations in a manner that is quite similar to the TRIPS Agreement rules. The existence of some intellectual innovation as a condition for originality in the author's selection of sources or in their organization to get copyright protection is mentioned in all three international accords. The World Intellectual Property Organization (WIPO) discussed and eventually delayed a proposal for a Database Treaty at its Diplomatic Conference held in Geneva, Switzerland in December 1996. The issue has remained on the agenda of WIPO's Standing Committee on Copyright and Related Rights (SCCR) since then, but little progress has been made due to growing resistance from poor nations [2].

The draft WIPO Database Treaty was based on European and American ideas that were comparable to the EU Database Directive in concept and scope. Although the database treaty was withdrawn from the conference agenda and the table, WIPO continues to work on the issue. The Problem of Originality in Database Copyright Protection The problem of uniqueness is the most significant consideration in database security. In normal life, answering the question "What is original?" is difficult enough, but in the setting of a copyright dispute, it becomes exponentially more complicated. It is often asserted that works are not sufficiently unique to be copyrightable. This is a crucial point since, regardless of the amount of labor required, work that is not unique cannot be protected. Before a court can evaluate if anything is original, it must first assess whether it is a 'question of law' or a 'question of fact.' This subject is riddled with inconsistencies and ambiguity. In the case of compilations or databases, however, copyright protection is limited to material provided by the author.' As a result, the compiler does not obtain any rights to the previously published information. Until 1991, the great majority of courts evaluated originality in compilations using one of two methodologies. Some courts praised the compiler's sweat of the brow' by determining that a compilation was unique due to the labor, time, money, and talent put into its creation [3].

Other courts held that the sweat of the brow' theory contradicted the fundamental precepts of copyright law and that compilations were unique if the compiler used ingenuity in the assembling and/or coordination of data. In Rural Telephone Inc v Feist, the US Supreme Court eventually put an end to the dispute in 1991, holding that effort alone can never be original in the constitutional sense. Instead, the Court decided that a compilation, like any other work, must demonstrate a "minimal degree of innovation" to be copyrighted. Feist outlined a three-step process for determining the originality of compilations. First, a collection of "pre-existing information, facts, or data" is required. Second, the information must be chosen, coordinated, or organized. Third, an original work of authorship must be developed as a result of such selection, coordination, or arrangement.

2. DISCUSSION

2.1Protection in India

There is no express legislation to protect databases in India. There is no specific regulation governing database security. Even though the Personal Data Protection Bill was proposed in Parliament in 2006, it has yet to be passed. The law seems to be based on the 1996 European Union Data Privacy Directive's broad structure. The law is structured comprehensively, to regulate the acquisition, processing, and dissemination of personal data. It's vital to highlight that the bill's application is confined to 'personal data,' as specified in Clause 2. Data protection is concerned with safeguarding the privacy of personal information, while database protection is concerned with safeguarding the creativity and investment made in the collection, verification, and display of databases. The Copyright Act of 1957 protects works in the genres of literature, theatre, music, art, and cinematography. Computer databases are included in the definition of "literary work." As a result, duplicating a computer database, or copying and distributing a database, is considered a copyright violation for which civil and criminal penalties are applicable.

The Information Technology Act of 2000 was recently revised to address cybercrime concerns. It has included two key measures that have a significant impact on the legal framework for data protection. Sections 43A and 72A are the ones in question. However, the regulations relating to data security and confidentiality are still insufficient. The proposed modifications broaden the scope of accountability for data security breaches and negligent management of sensitive personal information. There are just a few examples that may be identified in compilation works or databases [4]. One such case is Burlington Home Shopping Pvt Ltd v. Rajnish Chibber, the plaintiff advertised the mail order catalogs that dealt with many consumer items which were placed on a full list of the plaintiff’s clients. The given database was a costly one in a continuous process of assortment. The defendant got a copy of the database and started using it to constitutea relationship with the plaintiff’s customers. The issue that arose was whether a database dwelling onan assortment of mailing addresses of customers was a subject matter of copyright. The court held that the assortment of addresses involved devoting time, money, labor, and skill. Even if the sources are the same, assortment amounts to literary work to which the creator has a copyright.

In the case of The Himalaya Drug Company v Sumit, this was reaffirmed. In assessing copyright protection against infringement, Indian courts seem to endorse thesweat of the brow' notion or the skill, labor, and judgment test. The court held that assortment made by devoting time, capital, energy, and skill though taken from the same source concluded to literary work and was therefore protected under copyright. In Eastern book company v. Desai, it was observed that there should be a particular vision in the selection, arrangement, and coordination of contents in a database to allure copyright protection. Another person is

allowed to make a similar compilation but is not allowed to infringe upon the copyright of the previous compiler by using his fruits of labor. The court also observed that changing spellings, correcting typographical errors, and adding or eliminating quotes do not constitute a significant work to allure copyright protection in a compilation[5].

In other judgments, such as McMillan v Suresh Chunder Deb and Govindan v Gopalakrishna, the courts found that a compilation created by the dedication of time, money, energy, and talent, albeit being based on a common source, amounted to literary production and was therefore protected under copyright. The Court cited the US Supreme Court's Feist case, stating that a degree of innovation should be used in the selection, organization, or coordination of database contents to attract copyright protection.The limited safeguards for the database are as follows:

1. Article 21 of the constitution of India guarantees a fundamental right to personal liberty that includes the right to privacy.
2. Under IPC, the information stored in a computer falls under the definition of movable property i.e. corporal property, and is protected from data fact.
3. Indian contract act also protects by incorporating separate clauses for the confidentiality of the database.
4. Database protection under the copyright act, 1957.

This act safeguards works under literary, dramatic, musical, artistic, and cinematographic categories and computer databases. Thus, copying a database concludes withan invasion of copyright for which civil and criminal countermeasures are available. Hence, copyright protection for databases in India is safeguarded as collections under literary works. It includes works such as computer programs, tables, and compilations. The sweat of the brow theory or the skill, labor, and judgment test has been upheld by the Indian courts in concluding copyright protection against infringement. The courts have based their conclusion on the point that no one should be allowed to use for himself the fruits of another person’s skills [6]. The key issues in the copyright protection of databases are:

1. Digital Agenda
2. Downloading issue
3. The issue in computer-generated works
4. Protection of personal information in the database
5. Databases of abstracts of published articles

Electronic commerce has benefitted India significantly. With an increase in database bytes and memory and a reduction in the use of paper bundles, it has revolutionized the way offices and workplaces operate. A database is a meticulously set and organized collection of data, which may be written on paper or saved on any form of electronic media, such as a computer. Even though databases, such as telephone directories, must be collected as a result of a growing need in the normal course of business, the creators of countless electronic databases must bear the risks and responsibilities of gathering a large amount of raw data and then sorting it out using a competent search engine capable of facilitating information access. Investing in such databases is a typical practice in which whole companies are formed, with income coming from advertising, royalties, and subscription fees.

Pirates aiming to steal databases these days may use a variety of technological tools to recreate or clone any database and disseminate it across the globe, and they can do it for a fraction of the cost of producing such goods. As mankind grows more dependent on digital information and computers, as well as new technology gives more creative techniques to replicate and disseminate data products, such threats will only increase. The necessity for

enhanced protection was denied by some nations during the WIPO Standing Committee's Third Session. India agreed with the United States. The Indian delegation argued that concerns about the potential impact of database rights on research, science, education, and technological breakthroughs were unfounded and that current domestic copyright rules were appropriate and effective.

The Indian Copyright Act, 1957 was updated in 1994 to give more effective copyright protection to copyright owners by recognizing the separate class of computer programs as a kind of literary works and allowing protection of such computer-generated works. Amendments to the definition of "literary work" included works such as computer databases and other tables and compilations, as well as computer programs. The term "literary work" includes a "computer database," according to Section 2(o) of the Copyright Act.

The database's creators are relying on Indian copyright rules, which treat databases as literary works. Since India has ratified the TRIPS Agreement and the Berne Convention, innovation in the structure or selection of the database's topics is required to qualify for copyright protection. Furthermore, the Copyright Act specifies that copyright will apply to both traditional and creative works of authorship. The Indian courts, on the other hand, have not taken a firm opinion on the notion of creativity, and the Indian Copyright Act lacks a definition. Every issue is usually assessed based on the facts and circumstances specific to the case.

When it comes to evaluating infringement of copyright for databases, Indian courts have supported the idea of "sweat of the brow," which is often regarded as a measure of talent, work, and judgment. Courts have ruled in instances like Govindan v. Gopalakrishna, McMillan v. Suresh Chunder Deb, and others that a compilation formed by committing money, time, talent, and energy, even if derived from a common source, is a literary work and hence susceptible to copyright protection. The courts backed up their verdicts by noting that even tiny levels of innovation in a compilation were protected and that no one had the right to profit from someone else's hard work.

In a recent decision, the Delhi High Court declared that although another person may construct a comparable compilation, they do not have the right to steal the fruits of the prior compiler's labor and so breach their copyright. The Court decided that copyright rights must be granted to an original and unique technique of gathering facts, rather than to the inventive methods used to get those data. In the Feist case, the US Supreme Court decided that copyright protection requires a "modicum of innovation" in the coordination, selection, or arrangement of the things in the database. Finally, given the speed with which a technology revolution aspires to construct a worldwide environment, India must enact legislation that establishes the rights enjoyed by databases. Only properly defined copyright and database rights will nurture a legal climate necessary for the growth of electronic commerce in the absence of further protection for non-creative databases.

2.2Protection in the United Kingdom

The United Kingdom's European Reaction Feist sent off alarm bells throughout Europe. A Feist-style approach by European courts was feasible and would have constituted a significant danger to the European Union's database industry in particular. Because of the various originality criteria, the standard for database protection in the Anglo-Irish systems was quite different before the Database Directive came out in the EU. The United Kingdom has an extremely lenient approach to originality. Databases have long been protected by copyright as "collections or compilations of data" under English statute law. As stated in Peterson J's decision in University of London Press v University Tutorial Press, the criteria of

originality in this context was that some degree of 'labor, skill, and judgment' had been employed in theselection and arrangement of the contents of the work. It permits copyright in a database (as opposed to its contents), but only if the authorship is based on human intellectual originality. Where copyright exists, it is an author's right that will remain for the rest of his or her life plus 70 years. The Database Directiveextends copyright protection to databases as collections under Article 2(5) of the Berne Convention, without affecting the copyright protection of collections of works or materials arranged, stored, or accessed by non-electronic means, which are thus protected to the extent provided by the Berne Convention [7].

A database, according to Article 1(2) of the Database Directive, is "a collection of independent works, data, or other resources organized systematically or methodically and individually accessible by electronic or other means." A typical database system is made up of three different parts. The first is database-operating computer software, while the second is the actual data saved in the database. The Directive protects such information if it fits the criteria of "originality in selection or arrangement" (Recital 14), and the third component is a collection of electronic materials that enables the user to interact with the database to save, retrieve, and change data. Search criteria implemented in command strings or macro language operations, indexing techniques, thesaurus, and presentation methods are all included in this wide area. The Directive extends protection to techniques of display, manipulation, and data input in particular. In a radical departure from the copyright paradigm, the European Commission adopted a sui generis approach to database protection in Article 10(2), which grants the database creator the right to "prevent the unauthorized extraction or re-utilization" of its contents, in whole or in part, for commercial purposes, from that database. There are several exceptions to the right that are similar to, but smaller than, the fair use exceptions under copyright law. In this situation, the rightful owner must be from Europe, and in the case of a person, he or she must be a citizen or resident of one of the EU member states.

Because originality requirements are included in practically every copyright system known, the difficulty is exacerbated in the setting of compilations, where originality must be visible in the selection or arrangement of the items included. The Commission acknowledges that the database items are organized in significant part by the system. This standard is very similar to the one that was applied in the United States after Feist, with one exception: under the Database Directive, copyright protection requires intellectual creation by a human author, raising questions about the extent to which a database can be protected under copyright law if the data selection and arrangement is done by a computer program with minimal human intervention. The new right protects data from the time it is created until it is destroyed 15 years later Article 10(1). If the contents are substantially modified,' a new 15-year term may be acquired. The provision for a renewable sui generis right might continue in perpetuity if the contents are continuously updated, depending on what amount of expenditure is eventually necessary to be significant. However, the sui generis right is not absolute, and there are limitations to it. For example, a creator of a publicly accessible database cannot prohibit a legal user of the database from extracting or re-using insubstantial sections of it [8].

Furthermore, the sui generis right is susceptible to several exclusions for non-commercial purposes such as education, scientific research, and public safety. These exclusions are more limited than copyright law's related fair use provisions. For example, there are no exceptions to the sui generis right for criticism, news reporting, satire, or library usage. The basic goal of the intellectual property system is to encourage creativity and innovation while simultaneously preserving a healthy public domain. However, this new privilege may hamper the transmission of knowledge and its flow into the public domain. The final European

Commission Directive does not impose any conditions on sui generis protection, such as demonstrating a creative accomplishment or a unique addition to the prior art, which are the traditional justifications for legal departure from free competition. Rather, it just needs the database creator to show that "a considerable investment has been made qualitatively and/or quantitatively in either the acquiring, verification, or presentation of the contents.

Due to the commercial nature of facts, this may provide challenges for many groups such as academics, researchers, scientists, and students. Furthermore, there is a risk that the new database will be shut down indefinitely. Because the EC Directive does not give any further recommendations for determining the required degree of investment in either situation, this threshold will remain ambiguous awaiting judgments by European courts interpreting the yet-to-be-drafted local database laws. Furthermore, upon closer examination, the breadth of protection granted to investors under the hybrid extraction right seems to curiously surpass that afforded to writers of conventional literary and creative works under the Berne Convention's classical copyright paradigm. It misses, for example, the crucial difference made by copyright law between ideas (a legal metaphor for the non-copyrightable components of protected works, such as the facts or data they include) and the author's expression. This difference is generally applicable under the TRIPS Agreement to all copyrightable works, including borderline works like computer programs and factual compilations. The database legislation, on the other hand, makes no such difference. This implies that there is no increasing public domain substratum in the universe of data providers from which either research workers or second arrivals are gradually authorized to pull previously created data without obtaining licenses that may or may not be granted. Because the new sui generis regime lacks an analog to the idea-expression concept, investors effectively get proprietary rights in data as such, a sort of ownership that the copyright paradigm specifically prohibits. Sui generis proponents dismiss this possibility, arguing that other parties should be able to create their databases [9].

The scope of the sui generis database right was significantly limited by the Court's decision in this case. It defined the right's goal as the promotion and protection of investment in data storage and processing systems, drawing a clear difference between investment in producing data in the first place and investment in storing and processing it in databases. To claim a database right, it was essential to demonstrate a significant investment in the latter, i.e., the database itself, both qualitatively and quantitatively. So, when there is a significant expenditure in collecting and storage, the database right will still accrue. For there to be infringement, there must be considerable extraction and usage, including repeated takings that are insignificant in themselves. The EU and UK are the leading legislators in the realm of copyright. There are two rights in the UK's directive namely copyright and sui generis right related to database rights. The function of copyright is to protect skill and labor in managing a database and the function of the database is to protect investment which is needed for the development and maintenance of the database. These rights are independent of each other.

In 1996, The European Union to harmonize and provide security, passed the European Union Database Directive for the legal protection of databases. It allowed the database to be protected by a new sui generis right. This was implemented in the UK in 1997 and was called UK regulations. Before this Database Directive, there was no permitted definition of database and originality and only the case laws proved that the originality of the threshold was low. Thus, the database directive changed the position in two ways. 1) it gave a statutory definition for the database. 2) it gave a new originality threshold whose requirements have to be met by all the databases. The originality test under this directive is noteworthy due to its focus on creativity.

1. Article 1(2) defines a database as a store of autonomous works, data, or other materials arranged systematically or methodically, and individually accessible by electronic or other forms.
2. Article 4 says that the creator of a database must be a natural individual or a group of natural individuals or legal individuals.
3. According to Article 5, the creator of the database must have the right to authorize: Temporary or permanent reproduction of the whole or a part of a database in whichever way he wants. To authorize its translation, adaptation, arrangement, or alteration. To control the distribution of the database to the public but this right shall exhaust after the author himself sells the first copy of the database. To authorize its communication, display, and performance to the public.
4. Article 7(1) says that the member states must provide a right to the manufacturer of a database that shows qualitative or quantitative investment in obtaining, verifying, or presenting the contents of the database. According to Article 7(5), the extraction of vague contents of a database that detriment the legitimate interests of the manufacturer of the database must not be permitted.

In British horse racing board v. William Hill Organization Ltd.: BHB owned a database of the fixture lists. The William Hill bookmakers were given a license to use that information in betting shops but he used the data on its website and thus claimants issued proceedings for infringing the database rights. English court held that William had violated articles 7(1) and (5) of the database directive. ECJ on appeal held that to get protection under the database directive, the quantitative or qualitative investment in obtaining, verifying, or presenting the contents of the database must be shown and thus the horses and riders failed to meet these given conditions.

To show some investment to determine whether or not there is intellectual creation, the burden of proof is on the manufacturer of the database. Once it is done, the manufacturer becomes vested with the right of preventing its extraction or re-utilization. These rights are given for the starting duration of fifteen years plus an additional fifteen years for any kind of future investment that the manufacturer makes that results in considerable changes to the database [10].

UK data protection act gives 8 principles for legally protected data which are:

i. Fair and lawfully computed
ii. Computed for a limited purpose and in a manner consistent with those purposes.
iii. Sufficient, relevant, and not immoderate
iv. Accurate and up to date
v. Kept for a necessary period
vi. Computed in line with data subject’s rights
vii. Personal information is not to be moved to countries outside EEA without safeguards.

3. CONCLUSION

In India, there are different legislations for recognizing database rights whereas in the UK there is a European union directive database for recognizing database rights. The European Union Directive incorporates a reciprocity provision, which might negate Feist's influence. Databases of foreign origin shall only be protected by the right to prohibit improper extraction if the nation of origin affords equal protection to databases of European origin. International access to database technology allows devices like the reciprocity clause to apply

pressure on other nations' legal systems. Database protection advocates suffer a dearth of scientific evidence to back up their claims.

According to Maurer's research, the introduction of the EU Database Directive resulted in a one-time surge in the number of accessible European databases. The United States, on the other hand, has seen a continuous increase in the number of databases accessible while providing little security. The arguments against sui generis database protection seem to be winning. Computers and the Internet have changed the way the world operates, and these new technologies continue to benefit the globe. The capacity to access enormous volumes of data has improved as a result of this expansion. Establishing property rights over information goods by broadening the definition of property does not imply that an information monopoly would emerge. Legislators may instead employ property rights to strike a balance between private and public interests. The nature of what is to be protected and the activity that is to be forbidden are two components of the kind of protection. To pave a new path for database protection, the following pointers are suggested: I the purpose of a new database law should be to support commerce by providing a lead time to database producers for investing time, energy, and capital; (ii) a new database law should offer sui generis rights to non-original databases and copyright to original databases; (iii) a new database law should offer a mandatory system of a database registration. It is impossible to overstate the value of information and its preservation to inspire more individuals to contribute to the knowledge reservoir.

REFERENCES

[1] C. Yali, “The Protection of Database Copyright in the Era of Big Data,” 2020, doi: 10.1088/1742-6596/1437/1/012124.

[2] T. Ahmad and S. Dan, “Comparative analysis of copyright protection of databases: The path to follow,” *J. Intellect. Prop. Rights*, 2012, doi: 10.2139/ssrn.1839325.

[3] N. A. Manap, S. N. Hambali, and P. M. Tehrani, “Intellectual creation in database: A superfluous test?,” *J. Intellect. Prop. Rights*, 2013.

[4] A. Gupta, “Protection of Databases in India: Copyright Termination Sui Generis Conception,” *J. Intellect. Prop. Rights*, 2007.

[5] A. Mazumder, *Database law: Perspectives from India*. 2016.

[6] H. Saksena, “Doctrine of Sweat of the Brow,” *SSRN Electron. J.*, 2011, doi: 10.2139/ssrn.1398303.

[7] Y. H. Lee, “United Kingdom copyright decisions 2017,” *IIC Int. Rev. Intellect. Prop. Compet. Law*, 2018, doi: 10.1007/s40319-018-0681-7.

[8] M. Madhavan, “Copyright versus Database Right of Protection in the UK: The Bioinformatics Bone of Contention,” *J. World Intellect. Prop.*, 2006, doi: 10.1111/j.1422-2213.2006.00269.x.

[9] R. Clark, “Database Protection in Europe — Recent Developments and Modest Proposal,” *Data Sci. J.*, 2007, doi: 10.2481/dsj.6.od12.

[10] S. Strasser, “Copyright Law in the Digital Society: The Challenges of Multimedia by Tanya Aplin ,” *King’s Law J.*, 2006, doi: 10.1080/09615768.2006.11427648.

CHAPTER 6

CHANGES IN LAW RELATED TO CYBER CRIMES

Ms. Sakshi Pande, Assistant Professor,
School of Law, Presidency University, Bangalore, India,
Email Id-sakshi.pandey@presidencyuniversity.in

ABSTRACT:

Cybercrime is among law enforcement's most pressing problems, and various laws were enacted and/or changed to keep up with the evolving nature of cyberspace. Because of the flexible and encompassing character of virtual worlds, criminal acts inside them are more difficult to discover and halt, resulting in prolonged negative consequences for victims. Furthermore, the growth of online financing, e-shopping, and other internet activity puts society in danger since they demand people's delicate personal and financial information. As a result, it's understandable why cybercrime security is critical for a nation's social, economic, and safety aspects. To combat cybercrime, the Indian government passed the Information Technology Act of 2000. To keep up with the times, it made several changes, including changes to intermediary liability and offenses linked to cyberspace, like stalking and harassment. However, there are other issues about the implementation of these rules that must be resolved to build a well-monitored cyber environment. This article will analyze the situation and provide a quick overview of cyberattacks and cyberlaws in India.

KEYWORDS:

Cybercrime, Cyberlaws, Law Enforcement, Cyberspace, Online, Cyber Security.

1. INTRODUCTION

The deliberate targeting or abuse of a computer system or network to commit an unlawful act like deception, child porn, prostitution, security risk exploit, or cyberbullying is characterized as cybercrime. In the late 1980s, the very first incidence of cybercrime arose, corresponding with the fast development of email use. A spate of fraud arose when mail went viral throughout the globe and into the homes of people. The mail was portrayed as a real request for financial aid from a Nigerian Highness requesting to aid in the exodus of Nigerians, with the guarantee of millions of dollars being returned to the mail receiver.

After the introduction of Internet webpages in the 1990s, criminals developed new ways to gain access to a computer system via deception. Cybercriminals would spread viruses throughout the internet. The malware would then infect a webpage that a user visited later. After visiting the webpage, the virus could attack the user's computer. Another way to infect a user's computer was to display pop-up advertisements on a website they visited. If the users click the popup, their computer might be attacked with malware. Other viruses can slow down the person's PC or redirect them to a sexual website.

The internet brought a new age of social networks and internet entertainment in the early 2000s. The development of cybercrime reached a whole new level during this period. Following the development of social media, people started posting and spreading personal data. As a consequence of the storm of personal data gained from individuals, identity theft

took place. Additionally, the information might be used to get access to personal bank accounts, and also perpetrate bank card and accounting crimes[1].

During the first decade of this century, there were a variety of cyber-crimes, involving DDoS attacks on large websites, the SQL Slammer worm attacking the Database server, and multiple malware attacks.

2.DISCUSSION

2.1 Cyber Crime Classifications

The four primary types of cybercrime are as follows.

2.1.1 Individuals are the victims of cybercrime

Cyber attackers conduct crimes targeting a person or a group of people. The following are a few examples of cyber-crime perpetrated against people:

Email spoofing is a method that involves fabricating an email head. This suggests that the communication seems to have come from somewhere but is not the true or original source. Individuals are more inclined to accept an electronic message or mail if they assume it came from a credible source, so spam and phishing efforts often use these tactics.

Spamming: One sort of spamming is email spam, often characterized as junk mail. It's a bulk email communication that hasn't been requested. Spam first became popular in the 1990s, and it has become an issue for the greater part of users. Receiver email addresses are collected by spam bots, which are automated programs that scour the net for user accounts. Spammers use spam bots to create email distribution networks. In the hopes of receiving a few answers, a spammer will send mail to billions of email accounts.

Cyber slander: Cyber slander is the harm done to a person's image in the sight of others via the web. Making a derogatory comment is intended to harm someone's reputation.

Internet Relay Chat offense: IRC enables individuals from all around the globe to communicate with each other via a unified platform, also called a room. Cyber thieves primarily utilize it for meetups. Attackers use it to talk about their tactics. Child abusers use it to attract small kids. A few causes for IRC fraud include chatting to gain one's trust and then harassing one sexually, blackmailing individuals for money, and intending to publish the victim's intimate images or video online if the sufferer refuses to pay a bribe. Some are child abusers who abuse children for financial gain. Some individuals use IRC to gain money by posting bogus job postings and, on rare occasions, phony lottery tickets.

Phishing: Attackers try to get data such as access data or bank details by impersonating a reputable person through multiple mediums or via mail. Only a few instances include net blackmail, hacking, lewd conduct, trafficking, distributing, uploading, credit card forgery, harmful code, and other internet crimes against persons. Such a horrific act has the potential to do immense damage to a single individual [2].

2.1.2 **Property-related cybercrime**

1. Computer vandalism, intellectual offenses, online threats, and so on are examples of these sorts of crimes. The following are examples of intellectual property theft:
2. The illegal copying of software is known as software piracy.
3. Copyright infringement is described as when an individual or group's copyright is violated. It's also known as the unauthorized use of copyrighted items including audio, technology, and literature.

4. Trademark infringement is described as using a service mark or symbol without permission.

2.1.3 Cybercrime Against Businesses

The following are examples of cybercrime against businesses:

1. Unauthorized data alteration or deletion: Unauthorized viewing or copying of sensitive data without the content being altered or removed.
2. DOS attack: The hacker fills the victim's computers, systems, or connections with traffic in an attempt to overload the victim's assets and avoid people from accessing them.
3. Email bombardment is an Internet abuse technique in which a high number of messages are delivered to a specific email address in an attempt to overwhelm or overflow the inbox or server hosting the email address.

A Salami attack is also known as salami cutting or salami assault. The cybercriminals utilize an internet database to acquire customer information including bank details and card details in this assault. The hacker deducts very tiny sums from each bank throughout time. The hackers remain undiscovered since the customers are ignorant of the slicing, so there is no grievance made in this assault. Logic bombs, Trojan horses, data manipulation, as well as other cybercrimes targeting corporations are examples [3].

2.1.4 Cybercrime as a Threat to Society

Forgery: Fraud refers to the creation of a fraudulent document, signature, cash, or revenue stamp, among other things.

Web jacking: The term "web jacking" comes from the term "hijacking." Whenever the consumer taps on a link on the perpetrator's fake website, a webpage with the message appears, enticing them to open another link. If the user taps on the URL that looks to be authentic, he will be taken to a fake website. These activities are carried out to acquire accessibility or control over another's website. The layout of the victim's website might potentially be changed by the attacker.

Protection in cyberspace

While browsing the internet, bear the following in mind:

Do use a secure password and, if feasible, use two-factor verification in webmail. It's essential for keeping your email or social networking account safe.

Password protection guidelines:

A least 8 characters must be used in the password, with at least one smaller character, capital alphabet, numerical, and symbol. Substitute the character with a similar one. For instance, rather than O, we could use 0, and rather than lowercase l, we could use I, and so on. Things to avoid while creating a password include: Shouldn't use a passcode that is easy to guess. Private details shouldn't be used as a password, and repetitive letters must be prevented, as should using the same passcodes on several sites.

Two-factor identification

This is an additional layer of security that needs your login id and passcode, and an SMS confirmation code sent to your cell phone. Even if a hacker manages to break your passcode, he won't be able to login in the id in the absence of a temporary and one-of-a-kind confirmation code [4].

1. Never give out your password to anybody else.
2. Never communicate or exchange any personal details, such as bank account details, ATM code, or passcode, via an unencrypted link, such as email. Non-encrypted webpages are those that lack the lock symbol and https in the browser window. The "s" stands for secure, indicating that the site is safe to use.
3. If you are under the age of 18, do not join any social media sites.
4. Remember to update the operating system.
5. Visiting an untrustworthy webpage or clicking on a link sent by an unidentified or untrustworthy webpage must be avoided.
6. Shouldn't reply to spam messages.
7. Anti-virus must be installed.
8. When saving sensitive and confidential information, be sure it is secured.
9. Pop-ups might contain harmful malware. Whenever we agree or pursue the popups, background downloading occurs, and the downloaded file includes malware or harmful software. This is referred to as "drive-by downloads." Avoid pop-ups that provide site surveys on online marketplaces or other similar offerings since they might contain dangerous malware.

2.2 Important Cyber Laws in India

Cyber law is significant since it affects practically all elements of interactions and activities that take place on or involve the online, the WWW, and cyberspace. Each online activity and reply has certain legal as well as cyber law implications.

The world is growing and becoming more technologically advanced in today's modern techno-savvy society, as are crimes. The Web was created as a tool for study and data dissemination, and it was uncontrolled at the time. Through e-business, e-commerce, e-governance, and e-procurement, it got increasingly commercial over time. Cyber laws include all legal concerns relating to digital crime. As the number of people using the internet grows, so does the demand for cybersecurity and its implementation [5].

1. *IT ACT, 2000*
2. Section 43 - This section applies to those who destroy pcs without the customer's authorization. In such instances, the owner is entitled to full recompense for the total loss.
3. Section 43A has indeed been added to safeguard critical personal information held, dealt with, or processed by a corporation in a computer resource owned, controlled, or operated by that body corporate. When such a corporation is negligent in establishing and maintaining adequate security guidelines and rules, and as a result creates unlawful losses and gains to any individual, it will be responsible to pay penalties to that person.
4. Section 66 - This section applies if a person is determined to have committed any of the acts listed in Section 43 deceitfully or falsely. In such cases, the penalty might be up to 3 years in jail or a penalty of up to Rs. Five lakh.
5. Section 66B - Integrates the penalties for obtaining seized communication systems or computers in a dishonest manner, which affirms a possible three-year sentence. Based on the intensity, this sentence might also be followed by a fine of Rs. 1 lakh.
6. Section 66 D - This provision was added on the spot to concentrate on penalizing cheaters who use computer resources to impersonate others.
7. Section 67 of the Information Technology Act of 2000 has been revised to decrease the maximum sentence for publishing or sending obscene content in digital form from

3 to 5 years and to raise the maximum punishment from Rs. 1 lac to Rs. 5 lac. Sections 67A through 67C are included as well. Whereas Sections 67A and B cope with penalties for publication or transferring product that contains sexually explicit acts or child porn in digital mode, Section 67C offers an intermediary's responsibility to protect and maintain data for as long as the national government specifies, in the way and format that the central government specifies [6].

In light of the country's growing terrorist danger, the new revisions include a modified section 69 that gives the state the authority to make orders for the acquisition or surveillance, or decryption of such material via any computer system. Sections 69A and B, 2 additional sections, give the state the authority to issue guidelines prohibiting public entry to any data obtained through any computer system and to authorize the monitoring and collection of traffic data or information obtained via some computer system for cyber security.

Indian Penal Code

1. Those who commit crimes of identity theft or cyber fraud are likewise punished under the IPC Sections 379, 420, 464, 465, 468, 469, and 471.
2. Section 379 - Stealing is punishable by up to 3 years in prison and/or a fine. The above IPC Section plays a role because many cyberattacks are performed utilizing stolen mobile phones/computers or information theft.
3. Section 420 - Cheat and deceptively force property transfer. Cybercrimes such as the creation of fake internet sites and cyber scams are punished by a 7-year prison sentence and/or a penalty under this provision of the IPC. This part of the Code addresses offenses involving the theft of passwords to perpetrate fraud or create bogus websites.
4. Section 463 - Falsification of papers or electronic data. This clause makes crimes like mail spoof liable by up to 7 years in jail and/or a penalty.
5. Section 468 - Trying to commit fraud with the purpose to defraud carries a sentence of up to 7 years in jail and/or a penalty. One of the crimes punished under this law is mail spoof.

POSCO Act

This act makes it illegal to exploit a kid or kids for obscene purposes, including utilizing a child for sexual enjoyment over the world wide web. Persons guilty of the aforementioned offenses will be jailed for up to five years, and if convicted a second time, they will be jailed for up to seven years and penalized. The POCSO Act may also penalize anybody who keeps pornographic information featuring a child for the aim of profiting from it with up to three years in jail, a fine, or maybe both.

Despite the existence of cyber regulations, the prevalence of cybercrime is rapidly growing. During the year 2020, India had an 11.8 percent increase in cybercrime, with roughly fifty thousand incidents registered. Due to problems such as underreporting, criminal domain, awareness campaigns, and increased technical expenses of detecting crime, the police are struggling to solve cybercrime.

Even though there are several policies and rules dealing with cybercrime, there is a requirement to update existing laws as technology advances and criminals find new ways to conduct cybercrime. For successful cybersecurity, law enforcement organizations at both the domestic and global levels must work together more closely.

2.3 Case Laws On Cybercrime

1. The Bank NSP Lawsuit: This case concerned a bank management learner who was about to marry. The student and his fiancée mostly communicated via the company's computers. Both of them eventually went their ways. The girl, on the other hand, created a fake email account named "Indian Bar Association" and used the bank's system to send emails to the student bank's overseas customers. The bank lost numerous customers as a consequence of this behavior, and as a result, the customers filed a lawsuit against the bank in the trial. The bank was found to have committed the offense and was held accountable for sending the abovementioned emails to the customers because the bank was the origin of the messages.
2. Hackers gained access to the confidential information of more than 1.1 billion Aadhar cardholders after breaking into the Aadhar network in early 2018. Personal Aadhar card owners' information was leaked, according to UIDAI, and includes Aadhar, PAN, cellphone numbers, and Bank codes, among other stuff.
3. Cosmos Bank Cyber Attack: It included a cyberthreat on a Cosmos Bank branch in Pune. Because the hackers stole around ninety-four cr from Cosmos Cooperative Bank Ltd. in Pune, the financial sector in India has been shaken. The hackers who broke into the bank's ATM computer gathered data from a variety of Visa and Rupay debit cards. As soon as they acquired access, hacker groups from twenty-eight countries drained the accounts by withdrawing money [7].
4. Andhra Pradesh Tax Case: The owner of a plastics firm in the state was arrested, and the Vigilance Dept collected Rs. twenty-two from his residence. They requested confirmation of the cash that had gone missing. To prove the legitimacy of his deal, the suspect provided six thousand vouchers; but, a detailed analysis of the vouchers and the data of his devices indicated that each one was manufactured after the inspections. It was kept secret that the accused was running five firms under the appearance of one, and he had been falsifying sales numbers and avoiding taxes by utilizing phony and computerized vouchers.
5. As a consequence, when department investigators got laptops used by the defendants, the state businessman's fraudulent practices were uncovered.
6. Sony.Sambandh.com Case: The first cyber offense conviction in India has been reported. In this, a complaint at www.sony-sambandh.com was filed, a portal that primarily targets NRIs. Upon purchasing Sony items online, NRIs may utilize the service to send them to relatives and family in India. The business ensures that the merchandise will reach its intended audience. Someone going under the name of Barbara Campa went onto the portal in May 2002 and ordered a color tv and a wireless phone. She requested that the item be delivered to Arif Azim in Noida, then she gave her credit card information as payment. The credit card issuer approved the payment, and the deal was accomplished.

The products were supplied to Arif Azim through the firm after the completion of the appropriate due diligence and verification processes. When the goods were delivered, the corporation took digital photographs to prove that Arif Azim had received them. The purchase was finalized at that moment, however, the credit card company warned the firm after 1.5 months that the purchase was illegal since the true owner had rejected completing it. The CBI had initiated an inquiry under IPC Sec 418, 419, and 420 after the company filed an online cheat allegation. Arif Azim was arrested once the matter was investigated. According to investigations, Arif Azim received the credit card information of a U.S. citizen while operating at a contact center in Noida, that he used on the company's portal.

The color television and wireless phone were also recovered by the CBI. In this case, the CBI had evidence to back up its case, so the accused admitted his mistake. Arif Azim was found guilty under Indian Penal Code Sections 418, 419, and 420, making him the first person to be convicted guilty of a cyberattack. Since the accused was a 24-year-old 1st criminal, the justices ruled that a compassionate approach was warranted. As a consequence, the criminal was punished with a year of parole by the court. In certain circumstances, the IT Act's Sections 67 and 70 are also invoked. Hackers sneak into a webpage and replace the homepage with obscene or defamatory information in this scenario [8].

As a consequence of the emergence and spread of newly developed technology, many cyberattacks have been committed in recent times. Cybercrime has grown into a significant threat to mankind. Individuals all around the globe are growing more dependent on the web, which presents new opportunities for organizations and people that do not maintain their cyber defenses updated. In the coming future, cybercrime will undoubtedly rise. As a consequence of the risks associated with working at home and the potential for greater financial benefit, hackers will strive to ramp up their operations and create more complex and sophisticated methods of operation.

Bad actors are likely to continue propagating coronavirus-themed online scams and phishing schemes to capitalize on public concern about the epidemic. Corporate email compromise tactics are expected to rise as a result of the economic slump and change in the business environment, opening up new potential for criminal activities. The preservation of a nation's social, cultural, and safety components is all dependent on cyberattacks. The Information Technology Act of 2000 was enacted by the Government of India to tackle cybercrime. This Act also updates the Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Banker's Books Evidence Act of 1891, and the Reserve Bank of India Act of 1934 [9].

Crime may begin anywhere on the planet and go over national boundaries through the web, making it difficult to identify and prosecute these offenses on both a technical and legal level. Global harmonization initiatives, coordination, and collaboration among varied governments are required to prevent cybercrime. The major purpose of this publication is to provide the general public with information regarding cybercrime.

For the rising trend of cybercriminals, it is vital to get cyberlaw enforcing momentum since cybercrime can damage every aspect of life since it is simple to conduct but highly hard to detect. Despite India's extensive and very well legal system, all current laws were enacted decades ago, taking into consideration the significant political, societal, financial, and cultural conditions of the time. Back before, no one could have imagined what the Web would have been like. The needs of cyberspace could not be predicted, no matter how skilled our master draftsmen are.

3. CONCLUSION

The absence of knowledge on cyber cleanliness has been the most significant impediment to reducing cybercrime. Computer security has always been difficult to combat due to the absence of foundations and procedures. As a result, even once cyber-crime incidents are submitted to the police, nothing could be achieved. The Online demands a legally sound infrastructure that is up to date. Because current laws have failed to offer this legal framework, only the passage of appropriate Cyber laws would be capable to do so. All of these elements have conspired to make it easier for India to enact suitable cyber laws.

The government has created the National Cyber Crime Cooperation Centre with 4 expenditures to speed up examinations. An additional area where the nation's cyber security company might assist lower cybercrime levels is the growth of the country's cyber security industry. More funding in the sector may be able to tackle emerging threats with the launch of the 5G network as well as the creation of smart urban.

The world is becoming more reliant on technology, and the number of crimes using electronic devices is expected to rise. To reduce crime at a minimum, the country's law-making apparatus should strive to be a mile ahead of the criminals. As a result, governors and legislative bodies must make continual efforts to guarantee that regulating rules of technology include every part and problem of computer crimes and that they continue to develop in a continuing and healthy way to maintain constant surveillance and control over the connected crimes [10].

REFERENCES

[1] A. Soni, "Cyber Law in India," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2020, doi: 10.22214/ijraset.2020.1039.

[2] A. Sarmah, R. Sarmah, and A. J. Baruah, "A brief study on Cyber Crime and Cyber Law ' s of India," *Int. Res. J. Eng. Technol.*, 2017.

[3] D. A. Shaikh, "Challenges of Cyber Crimes and Information Technology Laws in India," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3551949.

[4] D. A. M. N. Deshpande, "A Brief Study on Cyber Crimes and IT Act in India," *Int. J. Trend Sci. Res. Dev.*, 2018, doi: 10.31142/ijtsrd18693.

[5] U. Pathak, "Cyber security and cyber laws in India: focus areas and issue areas," *Clarion- Int. Multidiscip. J.*, 2017, doi: 10.5958/2277-937x.2017.00008.9.

[6] D. A. Shaikh, "Study of the Cyber Crimes and the Laws Related to the Womens in India," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3551953.

[7] J. Shah, "A Study of Awareness About Cyber Laws for Indian Youth," *Int. J. Trend Sci. Res. Dev.*, 2016, doi: 10.31142/ijtsrd54.

[8] V. Kethareswaran, "An Indian Perspective on the adverse impact of Internet of Things (IoT)," *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J.*, 2017, doi: 10.14201/adcaij2017643540.

[9] I. Sharma and M. Afshar, "Privacy and Freedom Issues in Cyberspace with Reference to Cyber Law," *Int. J. Comput. Appl.*, 2016, doi: 10.5120/ijca2016910185.

[10] M. I. Ali and S. Kaur, "The Impact of India's Cyber Security Law and Cyber Forensic on Building Techno-Centric Smartcity IoT Environment," 2021, doi: 10.1109/ICCCIS51004.2021.9397243.

CHAPTER 7

ACADEMIC RESEARCH AND COPYRIGHT ISSUE

Ms. Ancy P Anto, Assistant Professor,
School of Law, Presidency University, Bangalore, India,
Email Id-ancyp.anto@presidencyuniversity.in

ABSTRACT:

Academic research is related to literary work and due to lots of similar research works, the chances of getting illegally copied raises concern. So, to protect from being an unauthorized copy of work Intellectual Property law gives protection by Copyright Act. For that, it provides a few essential criteria which need to be fulfilled. The guidelines are generally very common in all Countries. So, generally, any research work which is done gets protected easily in all countries. But if any person does not follow that guideline, then he or she shall not be protected by Copyright instead of protecting they get penalized. Copyright Act protects the author by prohibiting others to copy work without permission. As members of the legal fraternity judges, lawyers, academicians, researchers, and students continuously engage in legal research and writing, legal researchers and writers play a double role in their academic exercise as both creators and users of copyrighted materials. It means they have rights and duties regarding copyright law.

KEYWORDS:

Academic Writing, Copyright Infringement, Fair Dealing, Legal Research, Plagiarism.

INTRODUCTION

The primary object of protected innovation regulation is to convince the making of an incredible assortment of scholarly supplies. To accomplish this, the law gives individuals and organizations property freedoms to the data and scholarly merchandise they make, as a rule for a restricted period. Since they can procure benefits from them, this gives monetary temptation for their creation. These financial motivations are expected to animate advancement and put into the specialized advancement of nations, which relies upon how much security is conceded to trendsetters.

Copyright might be a right that allows the artificer of unmistakable work elite privileges for its utilization what's more, assignment. This is frequently common only for a limited time frame. The elite privileges don't appear to be outright anyway confined by constraints and special cases for intellectual property regulation, also as basically use. A primary limit on copyright is that it safeguards exclusively the particular articulation of thoughts, and not the hidden thoughts themselves.

The Copyright Act, 1957

The Copyright Act 1957 commands the subject matter of copyright law in India. The Copyright Act is in effect in India from 21 January 1958. The history of copyright law in India can be seen back to its colonialera under the British Empire. The Copyright Act 1957 was the first post-independence copyright legislation in India and it has been amended 6

times since 1957. The latest amendment was in the year 2012, through the Copyright (Amendment) Act 2012.[1]India is a member of the majority of the significant international conventions governing the vicinity of copyright law1 which includes the Universal Copyright Convention of 1951, the Berne Convention of 1886 the Rome Convention of 1961, and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). But India is not a member of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty

Fair Use in Education and Research

Segment 52 of the Act gives specific freedoms to the content clients including specialists to get to the material. While Section 14 of the Copyright Act enrolls the elite financial privileges of the copyright proprietors; Section 52(1) running from sub-statement (a) to (z) accommodates a few special cases for the elite privileges of copyright proprietors. While practicing fair managing privileges under Section 52, the clients need to regard the protected work and protect them from the dangers of copyright encroachment. They are permitted to utilize just a significant part. The idea of significance made sense later in this article. The fair management of the work implies fair use [2].

The intellectual property law of the UK utilizes the term fair arrangement whereas the USA intellectual property regulation embraces fair use. Indian copyright resolution utilizes the term 'fair managing' following the UK model. The TRIPS Agreement, 1994 additionally accommodates fair managing as restrictions and special cases. Article 13 of the TRIPS Agreement states that individuals will restrict impediments or exemptions to restrictive freedoms to specific extraordinary cases which do not struggle with an ordinary abuse of the work furthermore, don't preposterously bias the real interests of the right holder. Fair management regulation is fundamental for examination and scholastic reason, private reading, and the scattering of information. The term, fair managing is no place characterized in the Indian Copyright Act; henceforth, assurance of the extent of fair managing is to be done for a situation to case premise, which is generally a troublesome undertaking for the legal executive. The legal executive in India and abroad has created a few tests and tenets to decide if a specific debate is an instance of encroachment or an occurrence of fair management.

Three choices about copyright: retain it, share it, or transfer it

Retain it as an early Open Access copyright model

The Open Access Journal *Electronic Journal of Comparative Law* (*EJCL*) allows authors to retain their copyright and restricts reuse to educational purposes. *EJCL* was started in 1995 to create a scientific peer-reviewed journal with a good reputation in the electronic environment. Its copyright policy is simple:

1. The author keeps the copyright.
2. The copyright notice mentions that classroom use is free, but other uses depend on the permission of the authors themselves.
3. The journal asks only for a license to publish the article as the first publisher.
4. The author is obliged to mention *EJCL* as a source whenever the author later republishes the article on other platforms.

The copyright policy of *EJCL* is a good example of the copyright policies of many electronic-only Open Access journals that were started several years ago. These early Open Access

journals have frequently been published by the academics themselves without the involvement of a publisher or publishing organization. Leaving the copyright with the author spares the editors the trouble of answering permission requests.

Share it with a Creative Commons license

Creative Commons was founded in 2001, being in part inspired by the open-source software movement. Creative Commons has changed the copyright slogan "all rights reserved" into the slogan "some rights reserved," and has created various types of licenses whereby the creators can protect their works while still encouraging certain defined uses.

The leading Open Access journal publishers PloS and Biomed Central use the Creative Commons license 'attribution'. This license guarantees the author the moral rights – the right to be cited through a proper citation – but otherwise gives broad permission to use and reuse the article, including for commercial purposes. This type of license maximizes the impact of the research article on the author. A variation on this 'sharing of copyright' is seen in the journals of the European Geosciences Union. They use the Creative Commons 'share alike' license, which restricts the reuse to Open Access publications.

Transfer it (partly) - traditional journals that go Open Access

The *British Medical Journal* (*BMJ*) and *Nucleic Acid Review* are two prestigious journals that recently switched from the traditional model of publishing to an Open Access model. They use licenses that keep the copyright with the author, but the author transfers all commercial exploitation rights to the publisher. What does this policy mean? The *BMJ*, for example, leaves the copyright with the author, only requiring an exclusive license to publish the article first and claiming all commercial exploitation rights. The author retains all other rights to his or her *BMJ* article. In addition, the *BMJ* publishing group gives the author a percentage of the royalties if they enter into a commercial republishing or redistribution deal based on the author's article.

The advantage for authors is that they can do whatever they want with their articles without asking the *BMJ* publishing group's permission as long as commercial rights are not involved. The other advantage, of course, is that the model provides potential revenue for the authors from royalties: so far, this seems a unique approach in the world of academic publishing.

The Joint Authorship Doctrine

The law of copyright provides that an author is a person who creates a work of authorship and is at least the first instance, the sole owner of the work. Even though the author may initially have sole ownership of the work there are many methods by which the publisher may obtain ownership rights in the author's creative efforts. Two of the most frequently used are through the "work made for hire" doctrine - the publisher will own the copyright and "all" rights in the creative work-, and by an "assignment" of rights from the author to the publisher - the author specifically grants "all or some" of the rights in the work to the publisher.

When more than one person is involved in the authorship process the identity of the authors and the "rights and duties" of the authors may not be so obvious. The "joint authorship" doctrine involves a "sharing" of rights, although hopefully, especially if the publisher is a co-author, it is a deliberate sharing of rights and not an inadvertent loss of the publisher's complete ownership of rights in the work of authorship.

The Copyright Act provides for joint authorship when a work is prepared by more than one author "with the intention that their contributions be merged into inseparable or

interdependent parts of a unitary whole". If joint authorship exists, the authors of the "joint work" will be recognized as the co-owners of the copyright in that work.

The Importance of Joint Authorship to the Publisher

Co-authorship and collaboration are commonplace in the publishing industry. Examples of co-authorship and collaboration may include a co-writer, an illustrator, a ghostwriter, a book packager, or a work that includes copyrighted materials owned by another author or artist. When co-authorship or collaboration occurs several critical questions and issues arise. These include: Who is the author(s) of the work in the form in which the work will be published? Who is the owner(s) of the copyright in the work? Who decides when, where, and how to publish the work? Who receives payment or royalties for the work? The most appropriate time to resolve these matters is in a written agreement or agreement beforethe commencement of work on the project.

Right about now you are probably asking yourself the following question: "Why should the joint authorship doctrine be important to a publisher when its only impact is on authors?" You are correct in recognizing that the joint authorship doctrine only applies to authors, however, the reason this doctrine is important to publishers is that the publisher is the author of a work created as a work made for hire. Therefore, the publisher will be affected by the joint authorship doctrine if the publisher is not the "sole" author of a work created as a work made for hire.

One situation that may arise, where the publisher may not be the sole author of the work, is when the work is commissioned by the publisher as a work made for hire, but the publisher fails to satisfy the requirements of the work made for hire doctrine. If this occurs, unless the publisher has obtained, in a written agreement between the publisher and author, a grant of rights - including copyright ownership - to the work, the rights in the work would be owned exclusively by the author. The publisher, to prevent the loss of all its rights in the work, would have to prove that the work qualifies as a joint work and that the publisher was a co-author of the work. The publisher could prove that it was a co-author if the publisher acted as a collaborator in the work. One example of such a collaboration would be when an employee of the publisher or a freelancer hired by the publisher added copyrightable materials to the work made for hire; such as illustrations prepared by a staff artist within the scope of the artist's employment or by a freelance artist who prepared the artwork as a work made for hire that satisfied the requirements of the Copyright Act or by copyright assignment by the freelance artist to the publisher.

Another situation where joint authorship could arise is if the work is created in its entirety by employees of the publisher, but where a portion of the work was not created within the scope of an employee's job; an example of this could be where an editor was asked to write materials for inclusion in the work, and/or where the work was created outside the employee's normal work day and possibly at a location other than the place of employment, such as in the evening and/or on weekends at home. Under this scenario, the employee could claim that he/she was a co-author of the work. If the employee is successful in this attempt to acquire joint authorship the employee would be recognized as a co-author of the work.

The Rights and Duties of a Co-Author

Assuming the work qualifies under the law of copyright as a work of joint creation the co-creators or partners might apportion the privileges and obligations of crafted by initiation among themselves. Notwithstanding, since no conventional understanding is expected between the co-creators or associates a lawful relationship of joint initiation might happen

even without the goal of the separate creators to make a work of joint origin. In this manner, assuming no joint initiation understanding has been formalized it will be assumed that the accompanying standards will apply.

1. Every co-creator will claim an equivalent possession share in the work. This will happen regardless of whether one of the co-creators has contributed a more noteworthy amount of the work than the other co-creators.
2. Every co-creator will possess a "unified" interest in the whole work. This truly intends that assuming the distributing project comprises delineations and text that the craftsman and the author will each claim half of the whole work, i.e., the workmanship and the text.
3. Any co-creator, without the authorization of their kindred co-creators, may concede non-select privileges to the work to outsiders. Notwithstanding, a co-creator may just allow elite privileges to the work to outsiders if the co-creator gets the earlier assent of the other co-creators.
4. Every co-creator should record to the next co-creators for any benefits got from the abuse of the work.
5. A co-creator has the privilege to dole out his/her proprietorship share in the work to an outsider or to pass on his/her possession offer to his/her main beneficiaries.

Every co-creator will be qualified for equivalent origin credit for the work upon its distribution.

Publisher's Guidelines that may prevent the Fragmentation of Ownership Rights

Keeping these rules ought to assist a distributor in withholding full possession freedoms in innovative works of initiation.

1. Verify you have a composed concurrence with each of your representatives who make business-related works and different works that might be distributed by the distributor.
2. Verify you have an expressed "turn out made available" concurrence with all consultants and self-employed entities who make works that are intended to qualify as a "turn out made available." Make sure you satisfy every one of the prerequisites of the turnout made available regulation.
3. Incorporate a "task" of freedoms condition in the turn out went with for recruit understanding that will act as a back-up in the event the work neglects to fulfill the turn out made available prerequisites of the Copyright Act.
4. On the off chance that the work neglects to qualify as a turnout made available, work out, if conceivable, the safeguard of "joint origin" to forestall the deficiency of "every one of" your privileges in the work.

Judicial Interpretations

As expressed before, the Indian Statute doesn't official definition for the term fair managing. The fair management or fair use tenet started in the set of experiences as an adjudicator made the copyright exemption and later on, got legal acknowledgment. Indian legal executive likewise depends on pertinent unfamiliar points of reference on fair dealings as seen from the accompanying piece of this article. Ruler Denning in Hubbard and Another v Vosper and Another19 said accordingly: "It is difficult to characterize what is "fair managing. It should be an issue of degree. You should think about first the number and degree of the citations and concentrates. Might it be said that they are through and through such a large number and too lengthy to be in any way fair? Then you should consider the utilization made of them.

Assuming they are utilized as a reason for input, analysis, or audit that might fair arrangement. Assuming they are utilized to pass on similar data as the creator, for an opponent's reason, that might be uncalled for. Then, you should think about the extent. To take long concentrates and join short remarks might be out of line. However, short concentrates and long remarks might be fair. Different contemplations might ring a bell moreover. However, after everything is said and done, it should involve impressions. Likewise with fair remarks in the law of defamation, so with fair management in the law of copyright. The court of truth should choose." The Indian legal executive has talked about the issue of fair managing in various cases. In *Wiley Eastern Ltd. and Ors. v Indian Institute of Management*,[3] the Court decided that "the fundamental motivation behind Section 52 is to safeguard the opportunity of articulation under Article 19(1) of the Constitution of India so that exploration, private review, analysis or audit or detailing of recent developments could be secured. Area 52 isn't expected by Parliament to adversely endorse what encroachment is." In *Chancellor Masters and Scholars of the University of Oxford v Narendra Publishing House* [4] the Delhi High Court saw that fair managing precept ensures not just a public spot for swimming of thoughts and data, yet in addition an energetic public space in articulation, from which an individual can draw as well as renew. Fair use arrangements then, at that point, should be deciphered to figure out some kind of harmony between the selective freedoms allowed to the copyright holder, and the frequently contending interest of advancing the public space. The Court acquired four component tests from the American Pretty Woman case22 to decide if a specific utilization of a work is fair, and along these lines qualified for insurance under the fair managing exemption regardless of whether the utilization of the work truly falls under any of the classes referenced in Section 52. These four elements are:

1. The reason and character of the utilization (instructive purposes or evaluation and so on);
2. The idea of the protected work - whether the work is qualified for copyright insurance in the first place;
3. The significance of the piece utilized is comparable to the protected work - the degree and nature of replicating finished regarding a work; and
4. The impact on the expected market for, or worth of, the protected work - whether the new work would unfavorably influence the market worth of the first work.

Qualitative and Quantitative Tests

In R G Anand's case, the court saw that where the thought is formed alternately and the presence of dissimilarities can nullify a charge of encroachment, there can be both subjective and quantitative tests for finding the generosity however the strict number of words duplicated probably won't be the deciding variable for copyright infringement.23 If the 'core of the book' is taken via replicating that would add up to significant taking.24 For this situation, the zenith court alluded to numerous unfamiliar decisions to recognize fair managing and infringement.25

Verbatim Lifting

Word-for-word lifting is a clear instance of encroachment, which can't be managed at the cost of the protection of fair management. In *Syndicate of Press of theUniversity of Cambridge v B. D. Bhandari* [5] wherein the respondent had made word-for-word duplicates of the few concentrates from the Cambridge University distribution and counterfeited even the plan of activity, replies, and position subjects in his censured guide, the Court found it hard to term it as audit or analysis. Recognizing Syndicate of Press of the University of Cambridge from

Ramesh Chaudhry and Ors. v Ali Mohd,[6] the Court held that "an audit might sum up the first work and present it for the scrutiny to a third individual so a such individual might find out about the work. An analysis might talk about the benefits and bad marks of the work. An aide might look to empower the understudies of the first work to more readily figure out it according to the perspective of the assessments.

Word for word lifting of the text to the degree of duplicating the total arrangement of activity and the way to such activity can't be in any way named as survey, analysis or a manual for the first work." In Ramesh Chaudhry, the court had decided that "when the first writers of the books permitted the University to distribute it in their schedule and the University distributed it as a piece of their prospectus endorsed for its understudies, the matter went under the control of the overall population and no copyright in the severe feeling of the term stayed with the first writers. Having been distributed by the University, it turned out to be pretty much public property. Any individual from people, in general, could distribute an audit or analysis, or manual for this book." Blatant replicating of University endorsed books under the guise of 'guide' isn't allowed under the fair use precept. Word-for-word replicating of the first protected work for business benefits isn't permitted. However, audit, analysis, and distributing guidesare allowable under Section 52, autonomous.

Degree of Originality and Creativity

The quantum of skill, judgment, and labor required for copyrightability is not very high and what is the precise amount of the knowledge, labor, judgment, or literary quality which the author of any work including compilation must bestow upon his composition to acquire copyright cannot be defined in precise terms. Though there is no copyright in the ideas, facts, and information per se, how it is presented in a work makes it an original literary work. Hence, work on history is copyrightable, though the facts therein are not. A literary work need not be of any literary quality or merit. J Peterson in the University of London Press states that “the words ‘literary work’ covers work which is expressed in print or writing, irrespective of the question whether the quality or style is high. The word ‘literary’ seems to be used in a sense, somewhat similar to the use of the word 'literature' in political or electioneering literature, and refers to written or printer matter.” Researchers must be careful while dealing with new editions of old books as well. A new edition of an existing work is made by making additions, alterations, and deletions and if the changes made are material making the new edition original when taken as a whole, it is protected as a new work. As held in various decisions, many works which primarily appear to be so trivial for copyright are copyrightable and copyright exists in catalogs,[7] street directories, brochures, prospectus, index of railway stations or a railway guide, or a list of stock exchange quotations. One should be wary while dealing with collective and derivative works such as dictionaries or compilations, directories, etc. since these works are copyrightable. Database,[8] translated works, lectures, abridgment question papers [9], etc. are eligible for copyright protection. While taking information from these copyrighted materials, the researcher has to disclose the source accurately and sufficiently.

Copyright vis-a-vis Plagiarism

No copyright subsists concerning works in the common or public domain works. Hence, the researchers are free to use them. While using these materials, the researchers still have to respect the moral rights of authors under Section 57 of the Copyright Act. Under Section 57, the authors have special rights even after the expiry of the economic rights. These rights are inalienable and perpetual. In India paternity rights and integrity rights are recognized though the statute terms these rights as special rights of authors. Even after the expiry of copyright,

one has to acknowledge the source and respect the moral rights of authors, because it is demanded as part of academic integrity and honesty. One should not claim credit for something if it is not created by him. He has to disown what belongs to others and what he has taken from the public domain by giving credit to the original creators. The user must exercise sufficient caution to avoid the chances of committing plagiarism. There are theoretically several differences between copyright infringement and plagiarism. Copyright infringement takes place only concerning copyrighted work. Copyright is territorial and its acquisition is subject to statutory formalities, such as statutorily recognized subject matter,[10] works of original authorship, fixation, etc. Copyright is given for a specific period. When copyright exists for a specific period and copyright infringement can take place only within that duration, the perils of plagiarism would arise at any time. If ideas are not copyrightable, there can be plagiarism even concerning ideas. When copyright protects only expressions of an idea, allegations of plagiarism would arise if the researcher/writer fails to give credit to a person who has propounded a new idea or a phrase. Plagiarism occurs when ideas are copied without attributing the source. In copyright infringement, the permission of the author is required, if the fair dealing doctrine is not applicable. Copyright infringement and plagiarism may merge, when the researcher, copies somebody's work without authorization and pass it off as his work. The doctrine of de minims has no role in plagiarism. As stated earlier, while copyright insists on certain statutory requirements, these statutory formalities do not applyto plagiarism. One may not be imprisoned for plagiarizing someone's idea; however, academic dishonesty would cast a stigma on the persons' career damaging his reputation and integrity. When copyright infringement is a legal violation of the copyright holder's intellectual property rights, plagiarism is a moral wrong and academic offense.

CONCLUSION

Admittance to the protected material and new information is an absolute requirement for scholarly local areas to stay up to date with new turns of events and to make up and coming age of unique work. Admittance to information in itself is common freedom. Then again, security of the monetary privileges in the protected material and moral freedoms are likewise common liberties of the substance makers. These two rights are to be adjusted. The intellectual property regulation as a government assistance regulation attempts to adjust this. The special cases and restrictions joined to copyright are intended for safeguarding the public interest to approach the works and for the spread of information. Unapproved utilization of another person's work in opposition to the legal exemptions is not fair use. Fair managing is a significant exemption basically for non-business instructive and scholarly exercises. Since copyright depends on programmed assurance proviso under the Berne Convention,39 and no customs including enlistment are required40 separated from the negligible legal prerequisites, for the satisfaction and the activity of copyright, the clients and scientists ought to be very cautious. As scientists and journalists, individuals from the scholastic local areas must be cautious to safeguard their copyright in their imaginative works; simultaneously they have an obligation and obligation to regard the freedoms in the progress of others, who give them the structure squares to additional innovativeness. This obligation to regard creators and their works is a vital part of scholastic uprightness. Scholastic trustworthiness and genuineness go past the restricted time of legitimate copyright and any deviation from the said honesty isn't just a demonstration of counterfeiting but the mark of the end of scholarly innovativeness.

REFERENCES:

[1] Mishra J.P., "Intellectual Property Rights, Central Law Publications," vol. 23rd Editi.

[2] "https://spicyip.com/tag/fair-dealing." .

[3] *1995 IVAD Delhi 990, 61 (1996) DLT 281, 1995 (35) DRJ 522. .*

[4] "17 September, 2008."

[5] *3 August, 2011. .*

[6] "AIR 1990 Raj. 8." .

[7] "Diljeet Titus v Alfred A. Adebare, 130 (2006) DLT 330."

[8] *Blackwood v Parasuraman, AIR 1959 Mad 410. .*

[9] "Jagdish Prasad Gupta v Parameshwar Prasad, AIR 1966 Pat 33 and University of London Press v University Tutorial Press [1916] 2 Ch 601."

[10] *Article 5.2 of the Berne Convention, 1886. .*

CHAPTER 8

DEMAND AND THE RISE OF LEGAL TECHNOLOGY STARTUPS IN THE COUNTRY

Mr. Ranjeet Mathew Jacob, Assistant Professor,
School of Law, Presidency University, Bangalore, India,
Email Id-ranjeet.mathew@presidencyuniversity.in

ABSTRACT:

Legitimate advancement has generally implied the utilization of development and programming to help solitary lawful advisors, regulation workplaces, and medium and gigantic extension associations with preparing the chiefs, record storing, charging accounting, and electronic disclosure. Beginning around 2011, Legal Tech has created and associated more with development, and accordingly, new organizations have permitted people to web-based programming that lessens or on occasion clears out the need to guide a lawful counsel, or by interacting with people with lawyers everyone of the more beneficially through web-based business habitats and lawyer planning sites. Progresses in development, for instance, mechanized thinking licenses present-day programming to channel legitimate records, smooth out trades, and track down pertinent casework for lawful counsels.As of late, lawful innovation had certainly stood out as digitalization showed up with it. The staggering ascent of innovation prompted the groundwork of numerous new businesses across the world. It immensely changed enterprises and new businesses and took them to a higher level. Lawful innovation is the utilization of innovation to help the legitimate field in each perspective. This innovation is offering legitimate types of assistance to individuals utilizing the internet-based model. The motivation behind lawful tech organizations is for the most part to change the conventional legitimate field and its extension.

KEYWORDS:

Legitimate, Advancement, Solitary, Lawful Advisors, Digitalization.

INTRODUCTION

Technology has been evolving more than ever and ruling the world. Every sector of society has become dependent on technology and the legal field is no exception. Legal technology commonly known as legal tech refers to the use of technology and software to provide legal services, support lawyers by making their work less tiresome, assist them to provide legal service in a far quicker and more efficient manner, and make legal content more accessible to the common public. Technology in the legal field has given rise to Legal Tech Startups and these Startups are those companies that exercise technology and software as their method to provide all legal-related work through their online platform. Legal tech is quickly moving from the traditional sector to becoming a significant sector in the mainstream legal industry.

The evolution of technology is the significant reason for the formation of legal tech startups in India. The motive of these legal tech startups is to replace the traditional ways of procedural work which was followed by lawyers & other legal professionals with budding tech-driven things. Today's modern technology system has made it easier for lawyers to do

their jobs more accurately and very efficiently and as a result, it has benefitted the common public. The exceptional episode of Coronavirus has impacted the economy all around the world. As friendly separation was the best way to check the spread of the sickness in the public eye, the functioning society overall moved to the web-based mode. The pandemic left no area of the general public unaffected including the lawful area. Coronavirus caused an unsettling influence on the general set of laws, the obsolete adaptation of conveying equity and offering legitimate types of assistance. Generally, the standard cycle was to show up truly under the steady gaze of the court for hearing one's matter. Be that as it may, the pandemic has constrained the legitimate calling to depend on innovation. For example, directing virtual hearings or videoconferencing where advice and attorneys can seem online for their issues by sitting in their agreeable spaces. Legal advisors enjoy the benefit of directing gatherings with their clients and conveying answers to their clients on the web. The pandemic has changed the way regulation experts and lawyers work. It has carried better chances to change regulation organizations carefully [1]. Graduate schools have likewise gone advanced and changed to the internet-based method of education and understudies have acclimated to internet learning. Innovation has stayed in the top lawful associations as well as little legitimate firms and curiously lawful tech new businesses have likewise put resources into the equivalent. The pandemic plays had a significant impact and has given a huge open door to lawful tech new companies in giving legitimate help with each conceivable perspective. The pandemic has constrained the lawful business to improve and move towards computerized change and the business has excused itself to improve things.

DISCUSSION

Moving Away from Tradition

The legitimate innovation is planned to lessen the number of actual gatherings expected for client conferences. Usually, while the oppressed gatherings approach legal counselors for guidance about their challenges, present-day innovation permits them to meet on the web and whenever even while they are sitting at their PCs. This is where the regular law office's practices confronted a seriously large test on the lookout. A regular regulation office is clamoring with movement and maybe two times as much regulatory work where it takes around 18 to 20 hours for a legal advisor to set up a report in its entirety.[2]

This communicates the impact on trendy business people too. Legitimate tech new companies can give something interesting in contrast with immense, conventional lawful firms: adaptability, which empowers organizations to adjust their representatives' work processes, supporting the maintenance of ability and the excitement of worker commitment. As youthful, talented, and as of late graduated attorneys follow innovative pathways and vocations in legitimate new companies, this impact will logically end up being clear inside customary law offices' HR divisions.[3]

Regulation organizations are getting used to innovation

The developing interest in the utilization of such legitimate new businesses is clear from the way that law offices, which are not commonly connected with the speedy universe of tech new companies, are seeing the benefit of being close to the activity. Even though legal advisors have generally been marked as chance loath and, likewise, tech-disinclined, more associations are embracing innovation to further develop work processes and lift efficiency. To accomplish a strategic advantage, a few associations have shaped their advancement arms or joined forces with lawful tech firms. Inventive firms will generally beat their customary partners regarding execution, income, and client relations.

The advancement of legitimate innovation

Lawful innovation has developed into a basic part of rivalry among legitimate market substances. Different discoveries showing that legitimate innovation empowers attorneys to create reasonable and available imaginative arrangements and work in a happier setting, add to the writing on how the flooding request prompted the rise of new administrations and plans of action in the lawful business. Lawful tech organizations are popular in India since they give assorted and further developed choices like instruction, legitimate administrations, and innovative headways and assume a vital part in the economy's turn of events and progress.

Alongside that, they give a wide scope of legitimate administrations in a convenient, savvy, and proficient way, which benefits the clients as well as the firm. Weighty interest in this industry is additionally permitting lawful tech organizations to remain on the ball about development. "Legitimate tech is progressively getting cash from a few sources, including law offices themselves, private value, and investment reserves," Jim Leason, Vice President, Customer Markets at Thomson Reuters, expressed, "This energy has given new companies the fundamental lift to get their merchandise going".

Legitimate Tech and the Pandemic

The pandemic bound people in their homes, with a large number of individuals searching for online responses for their genuine issues. The issues ought to have been organized online because the working environment meets and genuine meets were denied. People under the impact of legal difficulty were looking for second real advice. These legal surprises included property questions, mercilessness against women, and discussions associated with isolated, and financial issues. Litigators have become accustomed to the elements of the courts over an extended time and have shown insurance from change. The rising of COVID-19, on the other hand, has obliged them to leave their respected practice and conform to the changes, giving gatherings from their homes. The pandemic has displayed that advancement is and not a decision but a need and ought to be seen as an accomplice.[4]

Therefore, the long-awaited digitization of authentic calling has finally appeared. Legal automated new organizations have arisen as a hero for people in some tough situ in these troublesome times, giving them a strategy for searching for an authentic course. The pandemic has obliged lawyers to rely upon development to give answers to their active clients. They began with video conferencing and have now reached out to consolidate a collection of extra authentic instruments.

Highly Demanded Legal-tech Start-ups:

1) **LawRato:** As one merits admittance to top-notch, proficient legitimate guidance from Top Rated Lawyers, LawRato is an intuitive web-based stage that makes finding and employing such attorneys in any city/court in India quicker and simpler. They are determined to make the legitimate experience exceptional by giving top caliber, financially savvy, and on-request lawful administrations for any need.They are not a law firm, do not provide legal services, advice, or "Lawyer referral services", and do not provide or participate in legal representation.
2) **Practice League:** Practice League offers different administrations to law offices and legitimate divisions all over the nation and the world. Lawful Contract Management Services, Matter and Case Management, IPR Management, and Document Management are only a couple of the administrations presented by the association. The firm gives lawful innovation answers for an assortment of areas, it is not legitimate to incorporate those that.

3) **SoOLEGAL:** The main private worldwide undertaking for regulation in the advanced domain it is a first-of-its-sort legitimate e-administration innovation stage, that offers start-to-finish administrations to attorneys, paralegal officials (CAs, corporate officials, and others), and law offices for improving, smoothing out, and supporting the productivity of individual experts and the training.

The stage gives an unmatched scope of administration to the lawful local area. Case/practice the board, record the executives, archive capacity, charging, invoicing, e-installment framework, CRM, a commercial center for clients to connect with lawyers, and legitimate cycle re-appropriating are only a couple of models. The webpage as of now has a huge web-based local area of individuals from one side of the planet to the other that are lawfully able to give skill.

1) **iPleaders**: iPleaders is a group of committed attorneys working to make the law more accessible to the general public. The courses are used by diverse individuals, ranging from attorneys and law students to consultants and the police. iPleaders believe that if businesses are adequately trained and provided with the necessary tools, they can manage their legal challenges.
2) **MikeLegal**: Asia's first AI-powered legal associate helping legal teams automate various processes to increase efficiency and make data-driven decisions. It has helped legal teams automate processes leading to less time on mundane tasks.
3) **Lawyer 24x:** They provide the best professional services at an affordable price. A team of experienced consultants will help individuals excel in their business goals and provide support at every step of their journey. Using AI, we can identify previously missed data (if any) which helps improve the quality of work. Lawyer24x has been helping start-ups & small businesses with company registration, trademarks, licenses, GST, and legal contracts since 2017.
4) **Legal Kart:** According to legal kart, it has launched quick legal advice, in which anybody may seek legal assistance from attorneys for as little as □249 and upwards. It was launched in December 2018. Furthermore, it has a nationwide network of about 5500 attorneys. According to the company, LegalKart got 25500 legal aid requests for legal guidance from 500 locations around the country.
5) **Presolv360:** Bhaven Shah, Namita Shah, and Aman Sanghvi created presolv360, a Mumbai-based digital start-up, intending to replace the traditional workings of the court by establishing a technology-backed system that would enable individuals to deal with the problem efficiently and at cost-effectively.
   It is an end-to-end platform where clients log in and file a dispute and choose their desired outcome. They try to settle disputes on average within 45 days.
6) **Spot Draft:** Since 2017, it has established itself as a platform that uses legal technology to enable businesses of any size to analyze, write, and manage contracts. It assists clients in putting their businesses on autopilot.

7) **Lawctopus:** It is a law student-oriented website that provides everything related to law schools, such as internships, paper submissions, competitions, moot courts, and various career opportunities.

The use of legal technology is beneficial not just to the general public but also to attorneys. Lawyers must be well-versed in technological advancements and adaptations. A slew of legal tech businesses has popped up in the market to provide consumers with legal tech services and assistance, bridging the gap between attorneys and clients. The widespread use of legal

technology is cost-effective, lowers the time it takes to offer specific services, and provides a better means for lawyers to interact with their clients. These companies are now well-known in India, and they are growing day by day [5].

Benefits of Legal Tech

A larger number of benefits are provided by legal tech, some of them are:-

1. ***Lower rate of risk***: As human beings we all make mistakes, Lawyers made mistakes too in citing facts of the cases, information related to parties, and many more. Which is somewhere that affects their reputation and also financially damages them. But due to machines, software chances of these mistakes reduce.
2. ***Reduce workload****:* Historically Lawyers were more concerned with paperwork (which is still) and everything is done on paper but now Lawyers can do their work on machines and store them for a longer period.
3. ***Help in researching***: As we know researching is one of the pillars of the legal field. Researching helps to gain more and more knowledge about the topics and researching also helps to create a strong base for a case. So Lawyers can defend their parties in court more effectively. Legal tech companies provide a wide range of research. This research also helps law students and layers to give a boost to their careers.
4. ***Transparency***: As we know some Lawyers mislead and complicate the case just to make more money from the client. Which somewhat affects the image of the organization. But this lawful put-into-practice managing emulsion gives transparency to the procedure of the organization.
5. ***Easy access to clients*** – Clients can easily access legal services through mobile software and other applications. It increases the direct communication between the client and the lawyer. The client can easily get information about the status of the case. This cuts needless paperwork, clients get meeting within a short time, and unnecessary physical meet also not needed. Through such innovation, everyone gets updated about legal matters. The client gets more satisfied.
6. ***Automation*** – With so many innovations in the field of law, more work becomes automatic for example, if there is a meeting or case hearing, then the lawyer can save the date for that and the application will notify them on time. Other examples are routine billing and file organization etc. It will save both time and money.

Legal tech can assist to change the Legal Field

Today innovation can be seen in every field and is made available to every individual. Hence, the legal sector must adopt the technology and change with time otherwise it will be left behind in the long run. Innovations in the field of law imply providing a helping hand to legal counselors, and law officers with n number of legal works and in turn also giving a chance to individuals to take help from the online counseling website. It reduces or diminishes the need to meet a lawyer face-to-face. The main purpose of Legal tech companies is to alter this traditional approach and make individuals more familiar with legal know-how.

The work of lawyers has become far quicker and more efficient as well with various technical tools, thus resulting in more profit [6]. Without the use of legal tech, the client might suffer in the short term but in the long run, it will be the lawyers who will suffer because ultimately the clients will choose other firms that are more aware of the advanced technology and are likely to deliver more cost and time-efficient results.

Thus, legal tech has assisted the legal field in the following ways-

1. The law firms have been able to break the barriers of traditionalists and become more flexible in their approach and have continually been motivating its employee, creating a happy work environment and thus, attracting newer clients.
2. The latest technology has enabled transparency, which helps the client to be aware of the progress made in the case and reduces their fear of being cheated.
3. Technology helps in the effective management of time and money, which means individuals, will have to pay lesser money to get their work done and the lawyers can take up more clients as their workload is reduced.

As a result of mixing law and the latest technology and software, a win-win situation is created for both lawyers and clients, thus improving their relations drastically.

Areas in which legal tech has proven to be helpful-

1. Contract management
2. Accounting
3. Billing
4. Document automation
5. Document storage
6. Legal research
7. Case management
8. Electronic discovery
9. E-signature platform
10. Practice management, etc.

Different tools provided by legal tech to deal with recent growth areas are-

1. Providing a platform to initiate conversation between the lawyer and the client.
2. Client relationship management tools.
3. Providing tools to enable individuals and businesses to deal with legal matters themselves avoiding help from the lawyers.
4. Law practice optimization
5. Data and contract analytics
6. Platforms for succession planning i.e. will be writing
7. The use of a digital signature helps to verify the digital identity of each signer.

8. Automation of legal writing or other substantive aspects of law practice.
9. Provide tools to deal with the preparation of immigration documents.

Legal tech and Indian judiciary

The judicial system in India was slowly moving towards digitalization and implementing technology in the system when the Supreme Court allowed live streaming of oath ceremonies and farewell speeches by judges. Further, a three-judge bench of the Supreme Court comprising Former Chief Justice of India Dipak Misra, Justice A.M. Khanwilkar, and Justice Dr. D.Y. Chandrachud allowed the live streaming of cases that were considered to be of national and constitutional importance.[7] Due to the pandemic, the judiciary has taken the virtual way to hear the matters and deliver justice. As technology creates a paperless environment it, therefore, provides an opportunity for the Judges to hear and determine the facts of the case with all the online available precedents and judgments in a fair, reasonable, effective, and timely manner thereby improving the administration of the judicial system. The Supreme Court is currently using the 'Vidyo platform for conducting virtual hearings. In July 2021, Justice Chandrachud said that all judges of the Supreme Court would be equipped with 1000 Mbps internet connection speed to avoid any disturbances which they would usually face [8]. Even during a pandemic crisis, technology has ensured that justice is not hampered, and with the assistance of technology, the legal system in India is certain to grow.

The first step to help individuals would be to perhaps set up products that make access to legitimate legal information easier. India's legal framework, laws, and rules are complex, elaborate, and difficult to understand for a layman. Easier access to laws will make it more convenient for an individual to understand and know their rights. Building a self-help bot using artificial intelligence models and Natural Language Processing as well as Machine Learning to train bots so they become efficient enough to understand the context of a question posed by a user, process its meaning and scope, and generate responses that will be helpful to guide an individual towards the right approach to a problem. While this product will perhaps not cure the legal system, it will perhaps help individuals filter litigious and non-litigious matters.

A computerized stage for people where they can have more modest issues, for example, challans/tickets given to them, little ticket purchaser assurance matters, protection claims, client assistance claims, little recuperation sums, and so forth would be a unique advantage. It won't just lessen the number of cases being enrolled under the watchful eye of the courts, however, will likewise give them the fast goal of their cases which would've if not required a long time to be settled.

A compelling, innovative innovation-driven circuit substitute question goal item would likewise make a huge effect. An all-encompassing innovation item that works with a biological system for all gatherings to a question goal including the petitioner, the respondent, and the impartial outsider middle person or referee. This item could give a safe store to records, a shrewd perusing of the issue articulation, guarantee, and realities close by, and utilizes innovation to recommend potential arrangements thinking about current realities, regulations material, and important legal points of reference.

The impact of innovation has been meaningfully altering how correspondence is done, exchanges are finished, and business is completed, and so on. Throughout some periods, innovation has affected varying backgrounds. While the development of the legitimate tech section has been slow and irregular in the Indian biological system, there have been significant advancements throughout recent years. With just 4% of attorneys involving any

sort of innovation in India, the requirement for better lawful tech cooperative energies is more noteworthy than at any other time.

With developing pendency, there is a critical need to find techniques that can assist with making ideal arrangements. While innovation is being utilized to deal with agenda cases through the case of the executive's arrangements, these improvements are simply a hint of something larger, with the immense utilization of man-made consciousness, AI, blockchain, and so on. It is maybe the ideal opportunity to utilize further developed advances and make research, and administration liberation, more intelligent, and more productive. Tracking down substitute strategies to determine debates utilizing innovation is certainly going to have an incredible effect. It is the ideal opportunity for legitimate specialists to wander into the innovation space, gather a more profound comprehension of how innovation capacities and track down inventive ways of incorporating regulation and innovation.

India's startup biological system has advanced at a huge speed, which has achieved creative change in the manner in which organizations work. One legitimate tech item that I predict being of incredible utilization would be agreement computerization and the executive's apparatus. As deals fill in the number, debates emerge as well. With better-drafted agreements, or arrangements utilizing blockchain to decide liabilities, secure exchanges, and trigger commitments better would be of incredible assistance to organizations. Paltry cases by either exploring specialists or questioning gatherings can be smothering for a developing business. Organizations are as a rule, ignorant regarding the idealness of an agreement and neglect to recognize conditions or viewpoints that could create problems for them later on, without lawful help. The greater part of them can't bear the cost of legitimate assistance and consequently, go into concurrences with stressing conditions that influence them later on. Moreover, the absence of understanding among exploring specialists of inventive plans of action additionally ends up being of worry, since the examination is quite often misled, which thus influences and seriously influences penalization of some unacceptable party. People are additionally influenced straightforwardly inferable from the absence of admittance to equity, which leaves them engaging with superfluous and delayed cases. India's intricate overall set of laws and far-reaching regulations likewise is a central issue for all gatherings required, since understanding liabilities and commitments becomes significantly more troublesome.

Future of legal technology

As technology is administering the world, every single area needs to be more technologically successful. It is assessed that products and machine will control the legal records. During the pandemic, most of the law offices shifted from disconnected work to online work. According to reports in the UK 48% of Law firms are utilizing man-made reasoning and the rest will do it in the future. A large portion of the work will be done through programming and machines like recording the board, a report investigating, and different works too. During the pandemic, case hearings were likewise done through video calls. Through this, it very well may be seen that the eventual fate of legal will help an ever-increasing number of advancements might be done in the legal field[9]. Legal new businesses are additionally going to be one such new company that will assist India with getting more advancement and will introduce the picture of India all the more unequivocally around the world[10]. A portion of the main legal techs in India is Ipleaders, Law Octopus, Vakilsearch, Vahura, MeetUrPro, Legal Kart, general law, Presolve360, and some more.

CONCLUSION

It's no surprise that the future of legal practice will increasingly rely on new technologies, with some sessions possibly taking place electronically. The sector will move beyond

traditional law practices or courts to some kind of diagnostic system that will advise consumers on their legal options, how to gather evidence, and provide alternative conflict resolution methods. Legal tech is a wanted element emerging into the legal sector that has rapidly transitioned from a niche market to a major player in the legal profession. Thus, technology law should be taken as a team sport promoted by all for the sake of all shareholders rather than a competition that must be instead. A game that we must all promote for the sake of our clients and the future growth of the industry.

REFERENCES:

[1] D. M. Osina, G. P. Tolstopyatenko, and A. A. Malinovsky, "Digitalization of higher legal education in russia in the age of covid-19," in *Lecture Notes in Networks and Systems*, 2021.

[2] "Why do we need Legal Tech? , The Legal Technologist, 19th March, 2018, https://," [Online]. Available: www.legaltechnologist.co.uk/why-do-we-need-legal-tech/.

[3] "Pandemic Raises the Relevance of Legal Technology, ie Law School, 9th December, 2020," [Online]. Available: https://www.ie.edu/law-school/news-events/news/pandemic-proven-technology-not-optional-lawyers-necessity/.

[4] "AJ Shankar, The Pandemic Might be the Tech Disruptor the Legal Industry Needs, Forbes, 8th February, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/02/08/the-pandemic-might-be-the-tech-disruptor-the-legal-industry-needs/?sh=2afada5d3a40."

[5] "7 Disruptive Tech-Legal Start-ups in India, the IMW Post, 7th December, 2016," [Online]. Available: https://imwpost.com/7-disruptive-tech-legal-startups-in-india/.

[6] "Legal Tech, https://en.wikipedia.org/wiki/Legal_technology."

[7] Devika Sharma, ""Live Streaming | Cases of constitutional and national importance to be live streamed;," vol. Supreme Co.

[8] Mehal Jain, "'New VC Platform for Supreme Court Soon: Justice Chandrachud says Tender awarded to best player', LIVELAW, July 12th, 2021," [Online]. Available: https://www.livelaw.in/top-stories/new-vc-platform-for-supreme-court-soon-justice-chandrachud-says-tender-awarded-to-best-player-177311.

[9] "Future of Law." https://www.lexisnexis.co.uk/blog/future-of-law/how-legal-tech-will-change-in-the-future.

[10] "Rising demand for Startups.pdf." .

CHAPTER 9

BUSINESS LAW AND ITS CONFLICT WITH TRADE SECRETS

Mr. Shinil Paul Mathews, Assistant Professor,
School of Law, Presidency University, Bangalore, India,
Email Id-shinilpaul.mathews@presidencyuniversity.in

ABSTRACT:

This paper discusses the necessity of trade secret protection and the many methods for doing so at both the national and international levels. To comprehend the significance of trade secret protection, one must first comprehend what a trade secret is and what information defines a trade secret. Some trade secret protection system elements will be offered that distinguish trade secrets from other IP forms, particularly patents, in that both protect innovations. Trade secrets are the foundation of all intellectual property rights and require extensive protection, as will be highlighted along with the importance of keeping information as trade secrets. This page also discusses trade secret protection at the national level, providing an overview of the various legislation adopted in various nations to protect trade secret information. Then it will be important to clarify what remedies are available to a person whose trade secrets have been violated or are at risk of being infringed in the future.

KEYWORDS:

Misappropriation,Patent, Property Rights,Trade Secret, Trade Secret.

1. INTRODUCTION

Organizations normally aggregate and utilize inventive as well as creative thoughts that are obscure to their rivals to acquire an edge over and keep up with the uniqueness of their items/administration. Data that isn't by and large known to contenders and is safeguarded by classification arrangements qualify as semi-licensed innovation known as 'proprietary advantage' and is qualified for security under misdeed or agreements regulation against revelation or unapproved utilization of the proprietary advantage. The size of a business is no criterion for the business to fit the bill for having a proprietary innovation and insurance for the equivalent. Upholding proprietary advantage insurance is exceptionally fundamental for the endurance of associations and fundamental for their endurance. In this time of globalization, organizations must guarantee that the security of their proprietary advantages from their rivals is sufficient in situations where there is the dread of divulgence, particularly while recruiting new workers for key turns of events or sending off new items and administrations. Proprietary advantage regulation's strategy is insurance, upkeep, and advancement of moral standards and fair management which empowers development, unapproved utilization of which by any individual who isn't a holder of the proprietary advantage is viewed as an infringement of proprietary advantages and uncalled for training.

1.1.Trade Secret:

A trade secret is any data or information about a firm that is not known to the general public and is kept confidential by reasonable efforts. "A trade secret is any knowledge having an economic value that is not in the public domain and for which reasonable efforts have been

taken to safeguard its secrecy," according to the North American Free Trade Agreement (NAFTA) [1]. According to the court in Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber [2], a trade secret is the knowledge that would cause actual or serious harm to the owner if exposed to a rival. It can include equations not only for product manufacturing but also, in some cases, the names of clients and the products they buy.

Three factors must be considered, according to Article 39.2 of the Trade-related Aspects of Intellectual Property Rights (TRIPS):

1. The information is not widely known among or readily available to those who deal with the type of information in issue, either as a whole or in the precise configuration and assembly of its components.
2. Because the knowledge is confidential, it has real or prospective economic value;
3. The person in legal possession of the information has taken reasonable precautions to keep it secret under the circumstances.

The Uniform Trade Secret Act of 1979, which was enacted in the United States of America, defines trade secrets as information such as formulae, patterns, compilations, programs, devices, and methods that:

1. Derive independent economic value from not being widely available or known to or easily ascertainable by proper means by others who can obtain economic value from its disclosure.
2. It is the subject of reasonable attempts to protect its confidentiality under the circumstances.

Financial data, customer lists, consumer information, and company goals and practices may be deemed trade secrets. Customer information, on the other hand, was not considered a trade secret or property in India. The goal of concealment was seen to be a benefit, hence a trade secret was created.

1.1.1. Judicial rulings for the protection of trade secrets

Trade secrets and sensitive information are not protected by law in India. Trade secrets, sensitive information, and commercial know-how all protectconsumer information, and company goals and practices radiation action can protect trade secrets generally. Trade secrets can be misappropriated through a third party's breach of confidence or unlawful access to privileged information. This misappropriation can occur either by misappropriating confidential information or by trickery or stealing.

The Indian Courts have streamlined three sets of circumstances in which proceedings may arise:

1. When an employee comes into possession of a secret or any confidential information in the normal course of his work and either carelessly or deliberately transfers that information to any unauthorized person;
2. When any unauthorized person (maybe a new employer) incites such an employee to provide him with such information as has been mentioned above; and
3. When, under a license for the use of know-how, a licensee breaches a provision, either expressly stated in any agreement or implied from behavior, to keep such know-how secret and fails to do so.

In the absence of legislation, Indian courts, and tribunals have made it very apparent that they will safeguard trade secrets through common law for the benefit of Indian firms. In John

Richard Brady and Ors v. Chemical Process Equipment P Ltd and Anr[2], the Delhi High Court held that it would be in the interests of justice to prevent the defendants from abusing the plaintiff's fodder production unit know-how, specifications, and technical information entrusted to them under the express condition of strict confidentiality.In *Daljeet Titus, Advocate v. M Alfred A Adebare and Ors*[3], the court agreed with the Duchess of Argyll and Ors [4] that the court must step in to prevent a breach of confidence regardless of the other party. Finally, the court instructed that the defendants would not be allowed to utilize the plaintiff's material that they had access to in violation of secrecy while issuing an injunction. The defendants who cooperated with the plaintiffs are barred from using the agreements, due diligence reports, customer contact lists, and other sensitive information they learned via their contacts. Concerning trade secrets of banking businesses, the Delhi High Court observed that banks owe a duty of confidentiality to their customers that arises from their monetary relations and that if someone steals such information that is guided by secrecy between such a bank and the customer, it shall be liable for obstructing such secrecy.

1.2.Under Contracts Law

Under the basis of justice and contractual obligation, Indian courts have maintained trade secret protection. The provision about restraint of commerce in Section 27 of the Indian Contract Act makes this clear. This provision, which is broad in scope, renders all trade restraint agreements unlawful. The provision was rigorous in its invalidation of restraints at first, but it was adopted while trade was still developing, and the section's purpose was to defend trade restraints. Later, the Law Commission of India's involvement in 1958 and its suggestion to allow reasonable restraint came into play.

1.3.Remedies for Infringement of Trade Secrets

In the event of infringement, an injunction or damages may be available. In India, the legislation of the Specific Reliefs Act, of 1877, may apply in favor of those who have been injured. However, a prima facie case must be proven, as well as a balance of convenience and irreparable damage. In several circumstances, an injunction has been denied owing to a lack of prima facie evidence. The courts have said that to obtain injunctions, the plaintiff must have concealed significant facts. Injunctions that cannot be precisely enforced by the court should not be given, according to Section 41 (e) of the special relief statute.

1.4.Trips agreement on trade secrets

Although Article 39 of the TRIPS Agreement permits parties to protect trade secrets, it only provides a summary rather than a definition. Article 39, paragraph 2 states that "natural and legal persons shall have the possibility of preventing information lawfully under their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as information:

1. Is secret in the sense that it is not generally known among or readily accessible to a person as a body or in the precise configuration and assembly of its components"
2. Has monetary worth due to its confidentiality; and
3. Has been subjected to fair measures under the circumstances, by the individual lawfully in possession of the facts, to maintain it.

The acquisition of undisclosed information by third parties who know, or were grossly negligent in failing to know, that such practices were involved in the acquisition is defined as "at least practices such as breach of contract, breach of confidence, and inducement to breach,

and includes the acquisition of undisclosed information by third parties who know or were grossly negligent in failing to know, that such practices were involved in the acquisition.

Article *l0bis* of the Paris Convention, on the other hand, which TRIPS members are required to follow under Article 2 (1) of the TRIPS Agreement and to which Article 39 of the TRIPS Agreement refers, provides general criteria for honest practices in clauses (2) and (3). Although clause (2) finds any act of competition that is contrary to fair trade practices in industrial and commercial matters to be unfair, clause (3) specifically forbids it.

1. Any conduct intended to confuse with a competitor's establishment, products, or commercial operations;
2. False claims made in the course of business intended to discredit a competitor's establishment, goods, or commercial activities;
3. Indications or claims that a trade is being used to deceive the public about the production method, attributes, purpose, or quality of items.

Trade secrets are covered under Article 39 of the TRIPS pact, which is an enlargement of Article l0bis. Article 39 defines any violation of secrets as a contravention, and so comes under the scope of Convention Article 106. Article l0bis, on the other hand, makes no mention of actions of unfair competition or illegal business activities. The World Intellectual Property Organization (WIPO) ruled in February that the use of classified knowledge constitutes unfair competition while expanding on the "Model Provisions against Unfair Competition" [5].

Article 6 of the Model Provisions, which is identical to Article 39 of the TRIPS Agreement, deals with trade secrets and determines when the use of confidential information constitutes an act of unfair competition. Paragraph (4) of Article 6 of the Model Provisions, on the other hand, deviates from Article 39(3) of the TRIPS Agreement and is directed at enterprises who exploit knowledge gained from authorities rather than the authority responsible for ensuring the appropriate security. Exploiting a secret without the owner's consent is unethical, even if the "owner" of the secret is unaffected. Secrets can also be obtained by authorization from the owner (e.g., a license) and independent discovery via "reverse engineering" based on observation of the object in public use or display. Indeed, releasing a product with an engineering secret on the market guarantees that the secret will be found first by competitors and subsequently destroyed.

Third parties that have legitimately obtained information but are not in commercial relationships with the authorized receiver of the information are not covered by Article 39. Third parties, on the other hand, will be held liable if they are aware of the sensitive nature of the data or if they are criminally negligent in failing to recognize that the data was obtained through deceptive business practices. Article 39 does not apply to third parties that have properly collected information but do not have a commercial connection with the authorized receiver. Third parties, on the other hand, will be held responsible if they are aware of the data's sensitive nature or if they are criminally negligent in failing to recognize that the data was obtained through deceptive business practices. Trade secrets are also protected by contracts. Trade secrets are frequently revealed by employees who break their employment contracts. [6] If information is disclosed in violation of a contract (e.g., a licensor-licensee relationship), a quasi-contractual relationship (e.g., a principal-agent relationship), or a relationship (e.g., an attorney, owner, or auditor), the law may be used to determine the contractual relationship's legal dimensions.

1.5.India's Landmark Cases

1. The major Indian case is *Konrad Wiedemann GmbH v. Standard Castings Pvt. Ltd* drew significantly on all of Lord Green's observations in the Saltman case. On the other hand, it is perfectly possible to have a confidential document, whether it is a formula, a plan, a sketch, or something similar, that is the result of the manufacturer's work on materials that anyone can use; however, what makes it confidential is the fact that the manufacturer of the document used his brain and thus produced a result that can only be produced by someone else [7].
2. Plowman, J. confirmed in *Suhner v. Transradio Ltd.* that the confidential existence of a document does not depend on whether the information it contains is available anywhere, but on whether it contains valuable information gathered for a specific purpose by the claimant, and if so, has been sent to the defendant for a specific purpose. If these requirements are satisfied, the record will be kept secret, and the defendant will not be allowed to utilize it for any other reason [8].

1.6.Protection of trade secrets under common law and worldwide

Under the system of free private enterprise and competition, the trader should gather as much knowledge about his rival's business as possible and share a bit of it with him. This knowledge might be a trade secret, such as a manufacturing procedure, or it could be a corporate, financial, or arrangement secret. Because it is possibly changing, some of this information would be exceedingly sensitive. Some would be less valuable if a competitor gained it, and much would be useless to a competing firm. Countries safeguard trade secrets as sensitive information. Where there are no special laws protecting trade secrets, common law protects them.

2. DISCUSSION

Normal regulations are uncodified. This implies there is no comprehensive accumulation of legitimate principles and rules which involves custom-based regulation. Precedent-based regulation is primarily founded on legal points of reference. These are kept up step by step through the court records and diaries, and reports. The uses of point of reference for each situation are not set in stone by the managing judges of the case. Proprietary advantages insurance is mostly founded on customary regulation standards. Proprietary advantages are being safeguarded under the agreement, semi-agreement, and property freedoms. The proprietary innovations insurance under agreement hypotheses incorporates which existed an express agreement or classified data and so on. The semi-agreement insurance incorporates evasion of out-of-line advancement from misappropriation of proprietary innovations. Proprietary innovations are viewed as a property right under the property hypothesis, which incorporates emotional as well as goal approaches subjects to defensive privileges in its purposes and exposures.

Under the customary regulation, the obligation for proprietary advantages misappropriation needs obtaining by one more by ill-advised lead or out of line implies and the utilization or divulgence by such individual to the weakness of the exchange proprietor. The domain for controlling the break of conviction has its beginning stage in the law of arrangement and worth because of the fix of request. The topic likewise possesses a similar moral territory as a break of trust. In this cutting-edge time, the breaking of certainty began in 1948 by engaging an English court choice in Saltman Designing co ltd v. Campbell Designing co ltd [9] For this situation, the break of certainty is considered as an alternate reason for the activity, and obligation exists withdrew from some other legitimate activity. Proprietary innovations and classified data are viewed as an impartial right above a property right in district precedent-

based regulation locales. On account of Coco v. A.N.Clark (engineers) Ltd [10], the test for recognizing a reason for an activity for the break of trust in the custom-based regulation world is set out. The court, while giving the directive, brought up, gave the test to a reason for an activity for a break of certainty as:

1. The data should contain the essential nature of certainty concerning it.
2. Data has been granted in the conditions committing certainty.
3. There should be unapproved utilization of that data, which thus is hindering to the party imparting it. On the off chance that the components of the misdeed of break of certainty are fulfilled, an activity can be begun for the genuinely upright proprietary advantages revelation under the misdeed of break. Courts give different cases to penetrate

2.1.Characteristics of the conduct

In Austria, the offender to be held criminally liable for trade secret violations must have acted at least with conditional intent. In Belgium, Estonia, and France, the conduct may be punished even if the offender acted with negligence. Cyprus does not establish any specific requirement that the offender must meet to be charged with criminal liability for trade secret violations. Nor is there any stated obligation on the owner to keep the information confidential. In the Czech Republic, the offender must act deliberately to commit the offense. As the relevant conduct is defined as an act of unfair competition, the offender must qualify as a competitor or someone participating in the competitive process. The concept of competition has nevertheless been construed very broadly, including even indirect or potential competitors. In Denmark, the offenses provided for under the Criminal Code require intent. Only upon certain circumstances, if the employee causes a substantial risk of dissemination of confidential information by negligence, he or she may be charged with criminal liability according to Section 19 of the Marketing Practices Act, without having acted with intent.

2.2. Fiduciary Relation Theory:

Fiduciary relations are generally based on the trust. The major aspect is the trust which operates such kinds of relations. This theory also has an impact on the employer-employee relation because, when there is no non-disclosure agreement in effect, then the information is deemed to be transferred under fiduciary relations. These fiduciary relations include the duty of confidence. Where an employee participates in the development of confidential business information, then he may also have some rights to such confidential information under the Common law principles; indeed, the employee may be the exclusive owner of such information. Even where the employer owns the information, courts may be less inclined in protecting the employer against the use (or) disclosure of the information by a former employee where the employee was the source or creator of the information. The English law of trade secrets is based on the idea that in given circumstances, the law implies that there is a duty of secrecy.

2.3.Misappropriation Theory

This theory is defined as an act of stealing confidential information from an employer and then trading securities based on misappropriated insider knowledge. In the United States, a person who is guilty according to the misappropriation theory will likely be convicted of insider trading.

The U.S. Supreme Court adopted the misappropriation theory of insider trading in *United States v. O'Hagan*

1. O'Hagan was a partner in a law firm representing Grand Met, while it was considering a tender offer for Pillsbury Co.
2. O'Hagan used this inside information by buying call options on Pillsbury stock, resulting in profits of over $4 million**.**
3. O'Hagan claimed that neither he nor his firm owed a fiduciary duty to Pillsbury so he did not commit any fraud by purchasing Pillsbury options.
4. The Court rejected O'Hagan's arguments and it specifically recognized that "a corporation's information is its property. A company's confidential information qualifies as property to which the company has a right of exclusive use.
5. The undisclosed misappropriation of such information in violation of a fiduciary duty constitutes fraud akin to embezzlement – the fraudulent appropriation of one's use of the money or goods entrusted to one's care by another[11].

In India, the Security and Exchange Board i.e., SEBI has banned insider trading and has laid down the **SEBI (Prohibition of Insider Trading) Regulation 2008.**There is no specific law for the protection of trade secrets in India. But the Indian courts have protected through various statutes, contract law, copyright law, etc., and also through the equity principles.**Section 72 of the IT Act 2000** provides for a penalty for breach of confidentiality & privacy.

2.4.Conflicts in the protection of Trade secrets:

There is a constant conflict between the fields of contract law & trade secrets which is unavoidable. It is expressed by the indiscriminate use of a non-compete clause in the contracts. Through this clause, the outgoing employees from the companies are restricted from being a competition to their employers. This clause causes a serious impact on the working & efficacy of employees. The Bombay High Court decided in Bombay Dyeing & Manufacturing Company Ltd. v. Mehar Karan Singh that the owner of a trade secret must take certain safeguards for the knowledge to be recognized as a trade secret.

Rule of Thumb

This rule states that to secure their information, businesses must adopt preventative and secrecy steps. These safeguards must be so evident that even strangers are expected to treat them the same way. If the owner of a trade secret freely communicates such knowledge, there is a risk that the information will lose its trade secret status [12].

3. CONCLUSION

Even though trade secret law fits into the current framework of tort law, contract law, and competition law, there are certain issues with its birth in the sphere of intellectual property rights. Separate trade secret legislation, on the other hand, would erase the gap. As a developing country, India requires a strong trade secret protection law. The TRIPS Agreement required that its Member States amend existing laws and enact new legislation to meet the TRIPS Agreement's obligations. It is past time for a statutory law to be enacted in India that protects trade secrets and confidentiality while simultaneously amending the existing framework of the Competition Act to prevent theft.

The country's criminal legislation, the Indian Penal Code, 1860, also has to be amended, as it currently does not provide for criminal culpability in cases of breach of confidence or disclosure of trade secrets, as it does in other countries. Individuals who engage in such

behaviors are not deterred by the mere presence of criminal law, thus extensive action and practice are also required to keep such instances at bay. Similar provisions in the Companies Act of 1956 should be updated to include due diligence concerning trade secrets. As a result, businesses may be proactive and cautious while safeguarding their trade secrets. Companies must develop a strong protective system around such information in this manner and for this purpose. Companies must also cultivate strong psychological loyalty among their employees for nondisclosure and/or non-compete clauses to be more successful, making it simpler to protect their trade secrets.

Taking the foregoing into account, it is reasonable to believe that trade secret protection in India is in its infancy and that it is critical for it to develop, keeping in mind that India, as a developing country, requires laws and legislation that are conducive to the business environment to transform the country into a hotbed of opportunities for companies offshoring as well as entrepreneurs seeking healthy competition.

REFERENCES

[1] *Article 1711 of NAFTA*. .

[2] *AIR 1987 Delhi 372*. .

[3] *130 (2006) DLT 330*. .

[4] *(1965) 1 all ER 611*. .

[5] "See, WIPO Publication 832(E) ISBN 92-805-0642."

[6] S. Sandeen, *Trade Secret Law in a Nutshell, 2nd edition*. .

[7] *(1985), (10), IPLR, 243*. .

[8] *[1967] RPC 329*. .

[9] *[1948] 65 RPC 203*. .

[10] *[1968] F.S.R. 415 (01 July 1968)*. .

[11] "https://supreme.justia.com/cases/federal/us/521/642/." .

[12] "https://indiankanoon.org/doc/286447/." .

CHAPTER 10

CYBERSECURITY IN ROBOTIC SYSTEMS: WEAKNESSES, THREATS, RESPONSES, AND SUGGESTIONS

Ms. Sakshi Pande, Assistant Professor,
School of Law, Presidency University, Bangalore, India,
Email Id-sakshi.pandey@presidencyuniversity.in

ABSTRACT:

Communication has evolved across the globe, particularly with the development of the Internet. The rise of cybercrime, often known as e-crimes (electronic crimes), is a major source of concern in today's society. Cybercrime, often known as software crimes, with the use of a computer to facilitate unlawful activity goals such as theft, child porn exploitation, theft of intellectual property, a stolen identity, and invading privacy. Crime is being committed through utilizing a computer connected to the internet to hijack someone's identity, as well as illicit imports or harmful software. Robots have grown more integrated than ever before in several areas such as agriculture, medicine, industry, army, enforcement (law enforcement), or logistics as a result of the current digital revolution. Robots are dedicated to serving, facilitating, and improving human existence. This involves intentionally hijacking or commanding robots, resulting in significant o monetary costs. This study examines the primary security flaws, dangers, and complications, and also the key security breaches in the robotics industry. Various techniques and suggestions were offered in this study to strengthen multi-factor device/user authentication techniques or multi-factor encryption algorithms to boost the security level of robotic systems.

KEYWORDS:

Cybercrime, Cybersecurity, Cyber Threat Intelligence (CIT) Internet of Things (IoT), Robotics, and Security.

1. INTRODUCTION

Cybercrime is known as any criminal activity that involves software, a device on the network, or a system. Although most cybercrimes were committed to making revenue for the perpetrators, certain cybercrimes are committed to targeting computers and other devices precisely to harm or destroy them. The Internet carries a vast range of linked networked computers that utilize the Internet protocol to communicate the “Internet of Things (IoT)”. The Internet has grown to be among the most important aspects of modern life. The internet serves 2 main tasks as a result of the information technology revolution. On the one hand, it has added good value to the globe. On the other side, technology has created a host of concerns that have undermined societal order and spawned a massive influx of crime around the world [1].

Individuals or groups with limited technical talent might engage in cybercriminal activities, and may fully coordinate worldwide criminal groups which comprise competent coders and those with specific knowledge. Cybercriminals typically seek to operate in countries with

loose or nonexistent cybercrime laws to reduce their chances of being identified and prosecuted. Cybercrime may start everywhere there is digital data, availability, or desire. Cybercriminals range from a single user involved in harassment to state-sponsored agencies such as China's intelligence agencies [2].

Cyber-attacks may cause power outages, the failure of weaponry or systems, and also the revealing of sensitive national security information. They might result in the theft of vital or highly confidential, like medical records.Hackers may impair laptop and phone connections as well as paralyze devices, rendering data inaccessible. It is not an exaggeration to say about cyber threats can impair the functioning of life support systems. Without a doubt, data theft is some of the most devastating cyber-attacks. Figure 1 depicts important cyber threats or a mixture of them based on the study. They are sometimes known as the Central Intelligence Agency (CIA) trio [3].

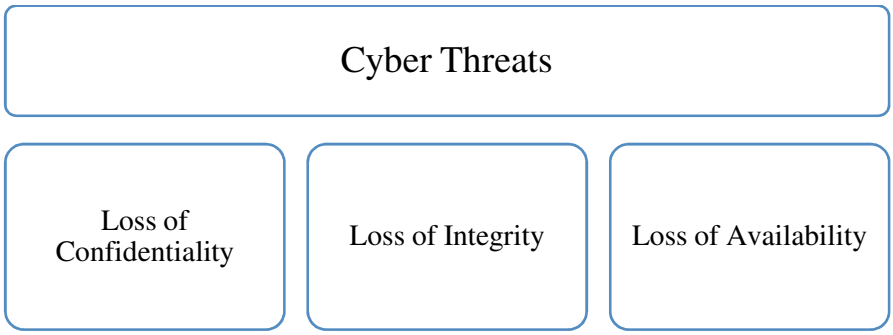

Figure 1:Representing the Different Cyber Threats or Central Intelligence Agency (CIA) trio.

1. Security breaches (confidentiality threats) can attack databases, backups, server software, or network administrators.
2. Theft, manipulating financial data, robbing huge sums of money, re-routing bank transfers, or tarnishing a company's effectiveness all of these are instances of integrity risks.
3. Availability (Denial Access) threats include targeted Distributed Denial of Service (DDoS), or physical injury.

Cyber-attacks were part of a bigger structure than what is often known as cyber operations. Data from any device integrated the use of comprehensive execution of electronic warfare, psychological operations, networking technologies, military deception, and also security controls in collaboration with specific assistance or necessary talents, to access, halt, dismantle, or hijacked human decisions and actions [4]. The architecture of a cyber-attack is depicted in Figure 2. According to the USNM Policy for computer network management, cyberspace operations consist of three components: assault, defense, or allowing use. The other differs from network assaults or network defense in that it emphasizes data collecting and analysis rather than network interruption, and that might be the precursor to an assault. Encryption is one sort of cyber-attack. Encryption is a reversing data encryption method that encrypts and decrypts the information using a password. Encryption and decryption may be employed in combination to provide an extra layer of security. Encryption is the activity and research of keys to encrypt and decrypt data so that only certain persons may interpret it. The technique for encrypting and decrypting data is the encryption method [5].

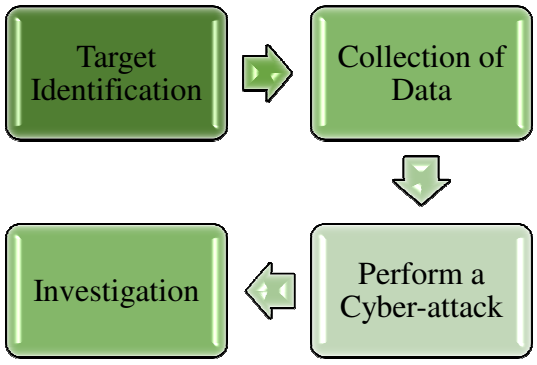

Figure 2: Representing the Architecture of Cyber-Anatomy Attacks.

Robotics is also one of those innovations that are seeing great expansion and progress, particularly in light of the current COVID-19 epidemic [6]. Certainly, robots play a significant role in civilized countries, providing several options for assistance in a variety of disciplines such as civil and armed sectors, and also agriculture, commercial, and healthcare. Furthermore, there are various worries with the use of robots in vital infrastructure (e.g. industrial, health care, and so on). These worries are mostly about privacy, security, reliability, or confidence. Security is mainly concerned with the amount of protection provided by these robots from various forms of cyber-attacks. The ability of these robotics to perform or substitute individuals in particular areas and actions determines their degree of happiness and capability to properly perform or substitute people in particular sectors and activities [7]. Significant security challenges, difficulties, risks, and threats emerge regularly, such as the illegal usage of these robotics through cyber-attacks, which might result in extremely serious death or harm.

The goal of this study is to emphasize the significance of using different robotic approaches (such as drones, robotics, submarines, AI, and so on) in all aspects of both the computing and networking worlds. Furthermore, the study underlines that the robotic realm faces some protection and stability issues that could result in harmful assaults. In this framework, the robotics potential threats, vulnerabilities, or assaults, as well as subjective risk analysis for these attacks are discussed. Equally important, they describe a collection of potential methods for dealing with these threats. Furthermore, the reliability and effectiveness of these methods are examined, as well as various recommendations are madeto improve the security of robotic systems. Finally, this paper provides a full review of robotic security, which is underrepresented in the sector.

2. LITERATURE REVIEW

Rajarshi Rai Choudhury et al. conducted a study that the most common forms of computer hacking reported to Inter-GOV were child pornography, forgeries, and e-mail abuse. Even more concerning are developing forms of cyber-terrorism made possible by the huge bulk of physical equipment being handled by computers. After trying to explain computer crime, this report analyzes the many forms that have already been committed as well as the new types which are expected to develop in the future. They also considered the difficulty of recognizing and measuring computer crime and also approaches for prosecuting and avoiding these acts and their effectiveness. This study analyzes the principles of computer crime, identification, or control. Furthermore, the study discussed the problems it brings to companies, the causes that support it, and potential solutions [8].

Jugoslav Achkoski and Metodija Dojchinovski proposed in a study that the goal of this work is to contribute to measures to combat cyber dangers such as cyber terrorism or cybercrime.

This also aims to demonstrate potential cyber security difficulties and rising dangers such as cyberwar, cyber terrorism, as well as cybercrime. Accelerating weapon development known as ICT (Information Communication Technology), which is being evolved at a faster rate every day, as well as raising human consciousness to a level higher about the consequences of ICT massive penetration, supports the establishment of emerging challenges in cyberspace. When a traditional weapon is compared to a digital weapon, it is clear that hardware represents assets that are utilized to launch bullets, whereas software symbolizes bullets that might cause damage or even have negative repercussions.

Modern risks such as cyberwar, cyberterrorism, or cybercrime pose severe disruptions in cyberspace security. Researchers may safely infer that even as ICT gets more advanced, the tactics and assets used in combating asymmetric threats, particularly cyber terrorism or cybercrime, would become more complicated [9].

Mariam M. H. Alansari et al. discussed in a study that communication has evolved across the world, particularly with the development of the Internet. Cybercrime, often referred to as e (electronic crimes), is a critical concern facing today's society. As a result, cybercrime poses a significant danger to authorities, businesses, and individuals worldwide.

It has spread throughout the world, and millions around the world have been victims of e-crime. Due to the magnitude of the crimes, their global breadth, and the consequences, it is clear that there is an essential need for a global understanding of these criminal activities to effectively deal with them. This research investigated the definitions, types, and invasions of electronic crime.This has concentrated on the laws that regulate e-crime in several countries. The research also includes cybersecurity or strategies for finding safety [10].

3. DISCUSSION

The following are the primary characteristics of this study:

1. The multifunctional usage of robots in numerous sectors places the groundwork for studying and evaluating robotic security assaults as well as their consequences.
2. To emphasize the many security weaknesses, threats, attack kinds, and other sources.
3. A comprehensive categorization of how assaults occur, including their impact, type, organization, as well as issues.
4. Present a set of guidelines and security standards to protect robots from such threats, reduce their harm, and therefore enable the relevant programs easier to design and maintain.

3.1. Areas of Robot Application:

Robots have been deployed in a variety of sectors and disciplines, including commercial and domestic applications, as seen in Figure 3.

The figure depicts diverse robotics applications for a range of activities and objectives in many domains of activities, including photographers, delivery process, agricultural production, wildlife conservation, police enforcement, search-and-rescue, emergency management, emergencies reaction, civilian death removal, reconnaissance as well as monitoring, counter-terrorism/insurgency, counter-IEDs/unexploded weaponry, border agents, construction safety checks, as well as scientific research. This section highlights the primary applications of robotics in the commercial, medical catastrophe, or agricultural industries, and also the military and police [11].

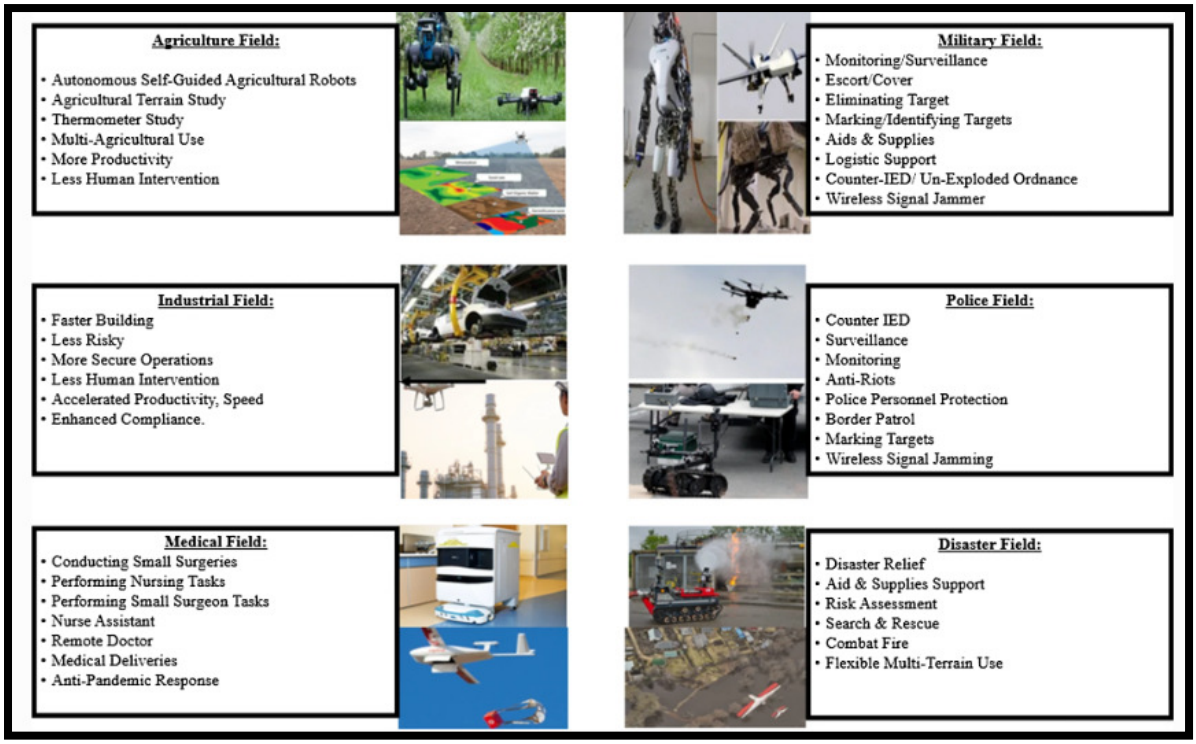

Figure 3: Illustrating the Use of Robotics in Agriculture, Military, Industrial, Medical, Police, and Disaster Fields[12].

3.1.1. Industrial sector:

Industrial robots are most often employed to minimize human labor. Robots have grown artificially intelligent, allowing them to do tasks more quickly, safely, and efficiently. Production, manufacturing, transport, and quality management are examples of these kinds of employment. Robots, in particular, are now being deployed in hazardous environments to do risky activities. They can also do repetitive jobs with more sensitivity and efficiency than their human companions [13].

3.1.2. Healthcare Sector:

In the medical domain, robotics have already been implemented for use in telemedicine, digital healthcare, or remote treatment ideas. They are created to be medicinal robotics, robotic surgery, or hospital robots. Robots are used to precisely execute minor procedures, and modern medical robotics were capable of executing Cardio-Pulmonary Resuscitation (CPR) [14].

3.1.3. Agricultural Sector:

Robots are utilized in agriculture because they are productive and efficient in reducing personnel or resource utilization. They are utilized to effectively complete various chores, especiallyinteracting with a huge farming region that needs at least a dozen personnel and many days. This helps with irrigated, crop testing, agricultural cultivation, and other procedures [15].

3.1.4. Disaster Sector:

Disaster robotics could be used to locate or assist defenseless persons who have been isolated by floods or who have become stranded and lost someplace. Disaster robots could do duties and get to regions where people cannot. Furthermore, robots have been deployed in the

firefighting sector, which aids in saving firefighters' life or having access to regions that have been determined to be too risky, too small, or too hazardous for firefighters. Following the tragic Beirut port explosion on August 4th, 2020, both robots or unmanned aerial vehicles (UAVs) are used, to assist in analyzing the destruction or effect area, and also in the hunt for missing people [16].

3.2. Taxonomies and Categorization in Robotic Attacks:

The goal of this part is to detect and categorize various assaults on both robotics and automation devices used. However, the significance of the attack is highlighted and investigated. Figure 4, summarizes the key robot-related cyber-attacks, their organization or effects, as well as their causes and issues. Finally, the primary risk assessment options are provided and analyzed to allow a faster evaluation of cybersecurity threats, hazards, vulnerabilities, or assaults, concluded by the proposal of a qualitative risk analysis.

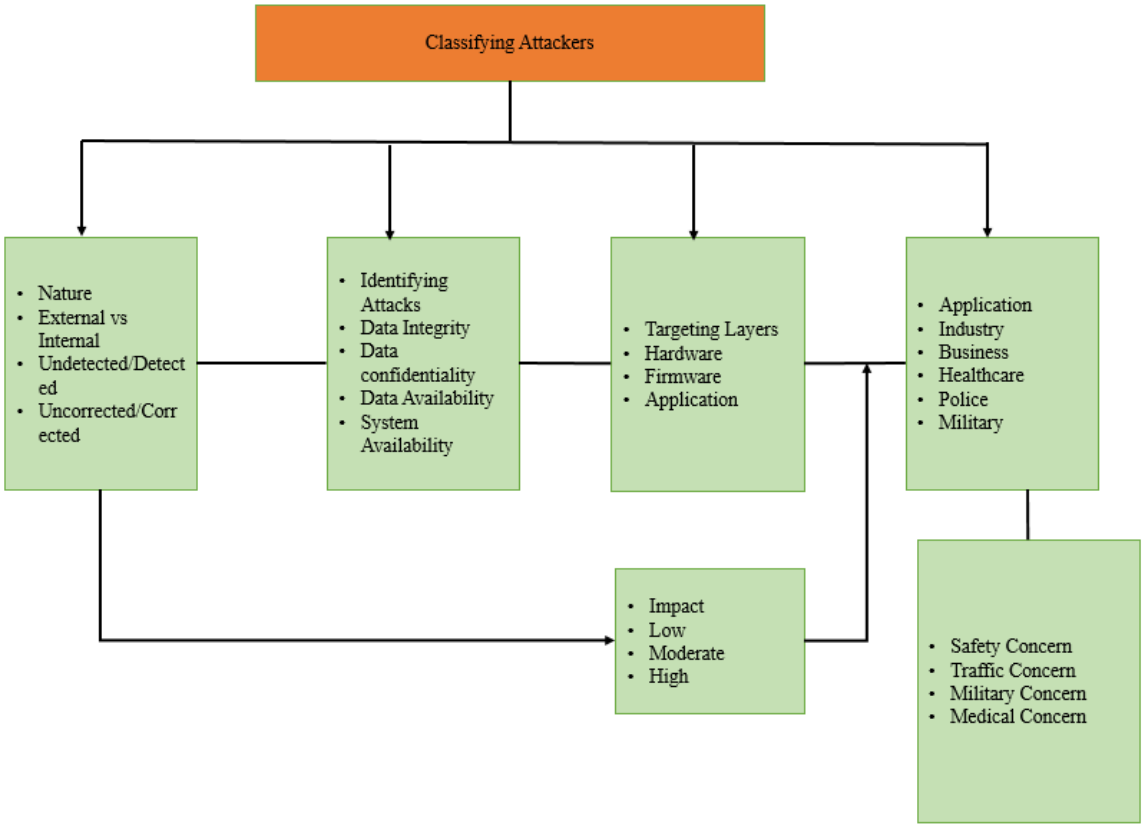

Figure 4: Displays the Outline of the Major Cyber-Attacks Involving Robots.

3.2.1. Hardware Attacks Against Robots:

These assaults can range from the least hazardous (such as fraud) to the deadliest (such as hardware). As a result of these types of assaults, backdoors might be created, allowing an attacker to launch another attack by getting unauthorized entry to the robots used or undergoing maintenance. In certain circumstances, they may have complete access to the gadget. However, robots were vulnerable to executing assaults such as side-channel attacks or failure attacks, which could result in significant loss of data and systems modification (based on the attacker's goals) [17].

3.2.2. Firmware attacks on robots:

Because of the availability ofFirmware passwords frequently preserved on flash drives, operating system (OS) modifications were accomplished by internet connection. Therefore, with every upgrade, the operating system may become exposed to new sorts of assaults. The operating system is vulnerable to DoS or D-DoS attacks, as well as misconfiguration extraction or root-kit assaults, according to the OS [18].

However, because apps rely on operating computer programs to accomplish the necessary functions, these softwareapplication attacks, expose the software to some dangers. This malware contains viruses, worms, and computer Trojans, as well as buffering overflowing or harmful cross-site scripting attacks.

3.3. Robotics Security: Proposed Solutions and Efficient Responses:

To safeguard robotics systems, appropriate security countermeasures must be implemented and maintained. As a result, identification and recognition procedures, and a strong multi-factor identification procedure (due to the strong identification and verification access policy or robot fingerprinting measures), were strongly recommended, in contrast to multi-factor security. This prohibits any potentially dangerous logical or physical unauthorized access. Safeguarding robotics, robots, and robot operating systems are indeed challenging tasks. As a result, it is not an insurmountable hurdle. As a result, several cryptographies, non-cryptographic, or AI-based methods for this task have been presented. The author emphasizes the many ideas given by different writers, as well as their benefits and consequences.

3.3.1. Intelligence on Cyber Threats:

The Cyber Threat Intelligence (CTI) idea is defined as information obtained regarding robotics dangers or dangerous people that would aid in minimizing damaging cyber-events through early management and detection depending on the Advanced Persistent Threat (APT) approach. Indeed, the dependence on CTI, particularly in distribution networks or Industry 4.0, enables a more timely and accurate alarm evaluation, enabling a more proactive and also reactive Incident Response Service (IRS).

3.4. Requirements For Security, Suggestions, or Directions For Future Research:

According to the examined studies, researchers discovered that further security standards must be investigated, performed, or assessed to improve the proposed protection mechanisms and suggestions for future study paths. A very constricted number of projects introduced should include trying to manage the security features of robotics during the design process, with much focus on how to sustain confidentiality Through the use of a strong cryptographic hashing framework as well as verification operating conditions Cipher-based Message Authentication Code (CMAC) and Galois Message Authentication Code (GMAC) are two examples (GMA), information is transmitted across encryption without regard for reference verification or encryption integrity.

3.5. Requirements for Security:

It is critical to adopt various security procedures to maintain the protection of robot wireless connections. This keeps communication safe while also ensuring authenticity, integrity, secrecy, or availability.

3.5.1. The security that Adapts:

To determine what data to safeguard or against which the information should be guarded, adaptive security systems may be separated into two categories: threat-centered or data-centered.

1. Threat-centered security analyses risks to implement the security mechanisms to save money, security precautions should not be installed if there is low danger. Provided an adaptable security system centered on threats.
2. This data-centric strategy guarantees that data sensitivity is assessed first, concentrating on which data has to be safeguarded rather than assessing the level of danger.

4. CONCLUSION

In the era of the internet, technology became an indispensable element of our everyday lives. If technology has many advantages, it is also becoming a menace to our life. To avoid being caught up in e-crime, it became vital to exercise vigilance when utilizing any technology. Robotic systems are now being implemented or utilized in a variety of critical infrastructure sectors. However, robotic systems have different security flaws which might be exploited to conduct deadly assaults, which can have severe implications for these infrastructures associated with economic losses of life. These assaults were conceivable owing to robotic systems' lack of security through design or dependence on open wireless communication systems. This involves identifying and blocking attackers from entering these systems to implant dangerous viruses and/or data, producing confusion and disaster within the operation of the robotics, or exposing vital information (industrial espionage). As a result, the authentication mechanism must be structured to provide the best level of security feasible by utilizing a user's mutual multi-factor authentication. This helps with minimizing unauthorized access to robots/users. Furthermore, privacy-preserving procedures should be utilized for a lawful person's privacy.Non-cryptographic alternatives such as prevention and lightweight detection systems must also be developed to further safeguard robotics programs. This study explored the security needs for robotic systems and made various proposals to meet those considerations. The authors want to shed further light on the major problems that have still to be conducted in future work, involving the development of anti-forensic measures to protect the authenticity of accessible information.

REFERENCES

[1] D. Itari, E. A. Anthony, and N. Mercy, "Cyber Space Technology: Cyber Crime, Cyber Security and Models of Cyber Solution, a Case Study of Nigeria," *Int. J. Comput. Sci. Mob. Comput.*, vol. 6, no. 11, pp. 94–113, 2017.

[2] S. K. Srivastava, S. Das, G. J. Udo, and K. Bagchi, "Determinants of Cybercrime Originating within a Nation: A Cross-country Study," *J. Glob. Inf. Technol. Manag.*, vol. 23, no. 2, pp. 112–137, 2020, doi: 10.1080/1097198X.2020.1752084.

[3] S. E. Donaldson, S. G. Siegel, C. K. Williams, and A. Aslam, *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats*. 2015. doi: 10.1007/978-1-4302-6083-7.

[4] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A Serious Game for Cyber Security Awareness and Education," *Comput. Secur.*, vol. 95, 2020, doi: 10.1016/j.cose.2020.101827.

[5] Z. ji *et al.*, "Harmonizing safety and security risk analysis and prevention in cyber-physical systems," *Process Saf. Environ. Prot.*, vol. 148, pp. 1279–1291, 2021, doi: 10.1016/j.psep.2021.03.004.

[6] P. Simoens, M. Dragone, and A. Saffiotti, "The Internet of Robotic Things: A review of concept, added value and applications," *Int. J. Adv. Robot. Syst.*, vol. 15, no. 1, 2018, doi: 10.1177/1729881418759424.

[7] M. Chui, J. Manyika, and M. Miremadi, "Where machines could replace humans-and where they can't (yet)," *McKinsey Q.*, vol. 2016, no. 3, pp. 58–69, 2016.

[8] S. Singh, "Cyber Crime against school children: Challenges & Solutions," *~ 264 ~ Int. J. Home Sci.*, vol. 6, no. 3, pp. 264–267, 2020.

[9] J. Achkoski and M. Dojchinovski, "Cyber Terrorism and Cyber Crime – Threats for Cyber Security," *Proc. First Annu. Int. Sci. Conf.*, 2012.

[10] M. M. H. Alansari, Z. M. Aljazzaf, and M. Sarfraz, "On Cyber Crimes and Cyber Security," 2019, pp. 1–41. doi: 10.4018/978-1-5225-8304-2.ch001.

[11] J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things (Netherlands)*, vol. 11. 2020. doi: 10.1016/j.iot.2020.100218.

[12] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocess. Microsyst.*, vol. 77, 2020, doi: 10.1016/j.micpro.2020.103201.

[13] "Industrial Robotics in Manufacturing," *J. Leadership, Account. Ethics*, vol. 18, no. 2, 2021, doi: 10.33423/jlae.v18i2.4258.

[14] J. Rosen and B. Hannaford, "Doc at a distance," *IEEE Spectr.*, vol. 43, no. 10, pp. 34–39, 2006, doi: 10.1109/MSPEC.2006.1705774.

[15] F. A. Auat Cheein and R. Carelli, "Agricultural robotics: Unmanned robotic service units in agricultural tasks," *IEEE Ind. Electron. Mag.*, vol. 7, no. 3, pp. 48–58, 2013, doi: 10.1109/MIE.2013.2252957.

[16] H. Mansour *et al.*, "Beirut Port Ammonium Nitrate Explosion," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3719078.

[17] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design and Test of Computers*, vol. 27, no. 1. pp. 10–25, 2010. doi: 10.1109/MDT.2010.7.

[18] R. Goyal, S. Sharma, S. Bevinakoppa, and P. Watters, "Obfuscation of Stuxnet and Flame Malware," *Wseas.Us*, pp. 150–154, 2013.

CHAPTER 11

AN ANALYSIS OF CYBERCRIME CASES IN THE MAJOR CITIES OF INDIAN STATES

Ms. Sakshi Pande, Assistant Professor,
School of Law, Presidency University, Bangalore, India,
Email Id-sakshi.pandey@presidencyuniversity.in

ABSTRACT:

Cybercrime is defined as any crime in which a communication channel or equipment, such as a laptop, desktop, mobile phone, and car, is used openly as a means of communication. Nowadays, the world is seeing a new generation of criminal behavior in cyberspace that is occurring internationally, independent of geographical boundaries. These cybercrime crimes might be motivated by money, include computer material, or aim to compromise the security, integrity, or accessibility of networked systems. As the number of users rises, so does the number of cybercrime occurrences, which do not respect regional or national borders and may occur anywhere in the world. Several examples of cybercrime have occurred in India in recent years; this is a critical topic of concern since it has a direct negative impact on people's social or economic life. This study focuses on the systematic examination of cybercrime crimes committed in violation of the Information Technology Act and the Indian Penal Code in India's most vulnerable states and cities. In addition, cybercrime incidents committed by people of various ages have been probed. Aside from explaining the many reasons for cybercrime activities and crimes, substantial remedial actions that must be taken to lessen cybercrime occurrences have been suggested.

KEYWORDS:

Cybercrime, Cyber Law, Cybersecurity, Indian Penal Code (IPC), Information, Technology.

1. INTRODUCTION

The Internet-based world of today has grown into a parallel way of life and existence. People can now do things they couldn't have imagined only a few years ago. For many individuals, the Internet becomes a way of life and also a way of living because of the increasing dependence on technology [1]. As such, cybercrime is described as any unlawful entrance into someone's computer system or database, the change or destruction of information kept online or on a computer, as well as the damage of hardware and information, all related to computer usage [2].In a broad sense, cybercrime refers to any crime committed on the Internet, including malware, terrorism, forgery, betting, cyberstalking, cyber theft, cyber pornographic, virus distribution, and so on. Cybercrime refers to any illegal conduct in which a computer serves as a device or a target or both.The majority of information in today's internet processing period is online and vulnerable to cyber danger [3].

Cyber laws, often known as internet laws, govern cybercrime. All legal and regulatory aspects of the Internet and also the WWW are covered under cyber law. Anything relating to or connected to or developing from any legal components or problems affecting any activity

taken by natives that those in cyberspace is referred to as "cyber law." [4].The use of a computer as a tool for illicit purposes, like forgery, smuggling in child pornography or intellectual property, snatching identities, or privacy invasion [5].The Internet domain, or cyberspace, is expanding rapidly, as are cybercrimes. Some examples of cybercriminals were listed below:

1. Crackers:

These people are out to cause harm, either for selfish reasons or for amusement. This category includes a large number of computer virus producers and distributors [6].

2. Hackers:

These people investigate other people's computer systems for educational purposes, out of interest, or to compare with their competitors.They may have the goal of gaining entrance to a more powerful computer, gaining recognition from other hackers, establishing a reputation, or gaining respect as an expert even though they have not had any professional education.

3. Pranksters:

These people are known for their pranks and pranksters. They are usually not aiming to do any long-term damage [7].

4. Career- criminals:

Although they are malcontents, addicts, and illogical and stupid people, these folks earn a portion or all of their money via crime. "When it comes to these folks, "they don't always commit violent crimes as a full-time job," says the author. After working a job, some individuals move on to the next one to keep the cycle of working and earning money. In other cases, they partner with other gangs or with organized crime groups such as the Mafia. "Russian, Italian, and Asian organized criminal gangs pose the biggest threat." In 1995, the FBI estimated that more than 30 Russian gangs were active in the United States. The FBI claims that "many of these nefarious partnerships employ modern information technology or coded conversations to avoid arrest [8].

5. Cyber Terrorism:

Cyberterrorism takes different forms.Also, a skilled hacker may get into a government site, and at other times, a large number of people with similar views could just flood the site with visitors. Addicts, alcoholics, competitors, and also criminally irresponsible are all prohibited from engaging in this activity.

6. Cyber Bulls:

The term "cyberbullying" refers to any sort of online abuse. Threatening forum comments, shouting out in chat rooms, making phone accounts on sites, or delivering cruel or rude private emails are all examples of cyberbullying in action [9].

1.1. IPC and IT Act 2000 Cyber Laws:

Almost all financial transactions on the internet, the World Wide Web, or Cyberspace are regulated by cyber law. It is the goal of cyber rules to establish a pattern and set of norms and criteria that may be used to classify diverse online business activities as either legal or illegal. Illegal actions were penalized according to the laws [10]. Traditional criminal behaviors like stealing, forgery, deception, harassment, or harm could all be considered cyber offenses under the Indian Penal Code. The Information Technology (IT) Act of 2000 tries to

modernize obsolete legislation and gives solutions to cybercrime. The introduction to the IT Act of 2000 specifies three goals [11]. To begin, legal authorization should be provided for electronic transactions. Second, to make electronic filing of papers with government entities easier, as well as third, to alter various Acts, incorporating the Indian Evidence Act of 1872 as well as the Indian Penal Code of 1860.

1.2. Penalties and Offenses:

Because there are several sorts of cyber-related offenses or offenses, the penalty meted out to the criminal varies according to the crime that was committed.Regardless of cyber legislation and government regulations, we may take numerous steps to reduce cybercrimes in the community. Below are a few ideas:

1. Confidential information of the respondents, email addresses, passwords, phone numbers, and so on must not be published on web pages.
2. Social networking platforms will not be used to publish photographs.
3. Unknown messages or users must not be replied to.
4. To safeguard the machine or information, use the most recent and up-to-date antivirus software.

2. LITERATURE REVIEW

Hemraj Saini et al. stated in a study that the majority of information in today's internet processing era is online andinsecure in the face of cyber threats.Because of the wide diversity of cyber threats, it is impossible to predict their behavior early on, making it difficult to minimize cyberattacks.

Cyberattacks may have a purpose, but they may also be carried out accidentally.Cybercrime is the word used to describe assaults that are conducted to cause financial harm, emotional distress, or pose a danger to national security. The prevention of cybercrime is predicated on a thorough examination of their behavior and also an understanding of the issues in all classes of society, As a result, this study gives knowledge of cybercrime and its effects on society, as well as future developments in cybercrime [12].

Lodh A and Dalave C stated in a study that with the rising number of COVID-19 incidents or fatalities globally, the entire globe is in a much worse state.Besides the Covid epidemic, the frequency of cybercrimes and cyberattacks of different kinds has increased worldwide.Although there has been a rise in cybercrime in recent years due to the rapid development of technology, the security protocols and preventative measures put in place to safeguard these advanced technologies and also the people who use them have not kept pace with these developments.

Therefore, the purpose of this study is to investigate and gain knowledge regarding the many different types of cybercrimes and cyberattacks which take place all over the world today.It is critical to prevent and raise knowledge about the many forms of crimes or assaults. Maintain your software updated, use anti-virus protection as well as a firewall, change your passwords frequently and keep them as strong as possible, and then use 2 or multi-step verification wherever appropriate.

Quwaider Muhannad et al. discussed in the study that this would address various economic and social elements as well as data analysis connected to phishing assaults utilizing neural networks. Authors investigated neural networks that gather data on phishing assaults to better

recognize patterns and decrease attacks. The authors determined that the precision is 89 percent, In addition, the COVID-19 pandemic's breakout is a notable aspect of the cyberattacks [13]. Hamid Zolfi et al. present in the study that this study described how to build a system for classifying cybercrimes in cyber-attacks. The dataset comprising data on cyber-attacks at the petrochemical firm was briefly discussed. Following that, preprocessing and normalizing were addressed and put into practice. Rapid Miner, as described in the preceding sections, was utilized for execution.Support Vector Machine, Nave Bayes, Decision Tree, or regression models were utilized to develop the methods, accordingly. The top classification method was the Support Vector Machine which had a precision of 99 percent and provided adequate accuracy for cybercrime categorization in cyber-attacks [14].

Shefali Batra et al. proposed in a study that no matter where one travels in this current age of technology, the globe is greatly reliant on technology. Because we relied on technology, thieves have taken advantage of this. Cybercrime is swiftly becoming the most rapidly growing type of modern crime. Cybercrime is well recognized for causing the demise of several businesses, personal identities, or organizations.It is the primary objective of their work to define cyber criminals, different kinds of cyber criminals, cybercrime as it affects the world, and how to avoid it.

This study also examined quantitative data on various forms of cybercrime and also its recent increase [15]. Priyanka Datta et al. stated in a study that the Internet and computer systems play an important role in modern civilization. People have significantly profited from the advancement of networking and cyberspace; however, some people are abusing this advancement to gain illicit advantages. Users of social networking websites have recently observed many sorts of social networking assaults. Internal Revenue Service (IRS) impersonator frauds, as well as technical support scams, seem to be the most popular types of trickery employed by attackers on unsuspecting victims to get financial rewards. The rate of cybercrime in India is always increasing for some reasons [16].

3. DISCUSSION

The information was obtained from many sources, study materials, or newspaper articles used throughout the current investigation. Some related literature was discovered, wherein the relevant data was gathered shown in Figure 1. The data for the study was gathered from secondary sources such as websites, journals, papers, questionnaires, and reports.

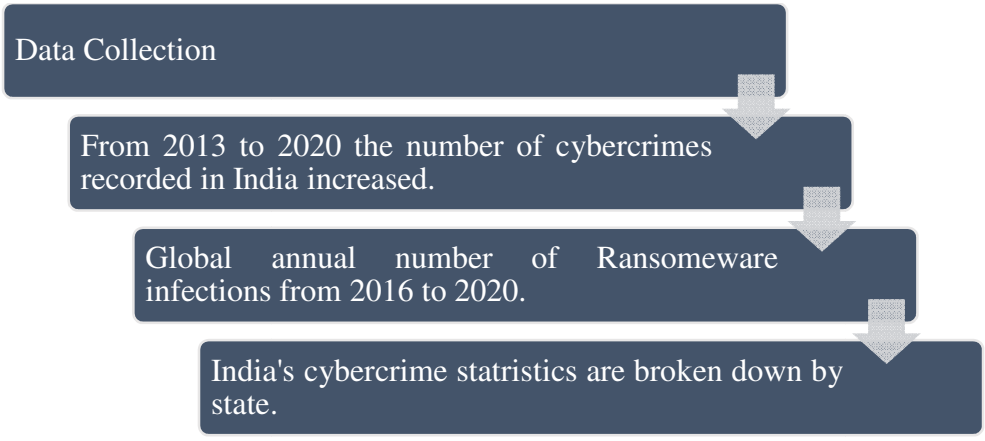

Figure 1: Depicts the Flow chart of the Cybercrime Cases in India.

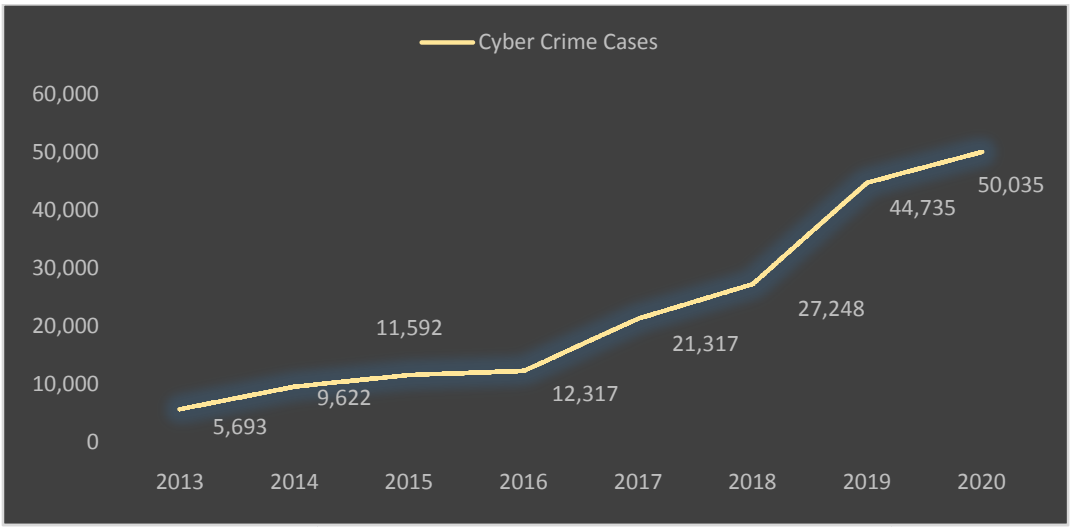

Figure 2: Shows the Frequency of Cybercrimes Reported in India Grew Between 2013 And 2020.

According to government statistics, cybercrime incidences in India increased at a quick speed, approximately tripling between 2013 and 2020.India's 'Crime in India' study estimates that by 2020, cybercrime in the country would have grown from 5,693 instances in 2013 to a projected 50,035 occurrences.

Furthermore, the number of incidents increased by roughly 85 % between 2018 and 2020. In 2018, India logged 27,248 cybercrime incidents. Furthermore, the number of reported cases in 2020 was roughly 12% higher than in 2019 44,735 instances shown in Figure 2. Research conducted every year on the state of cyber security throughout the world found that there were 304 million malware attacks worldwide in the year 2020. It was the second-highest quantity since 2016 and represented a 62 percent increase in comparison to the previous year's total shown in Figure 3.

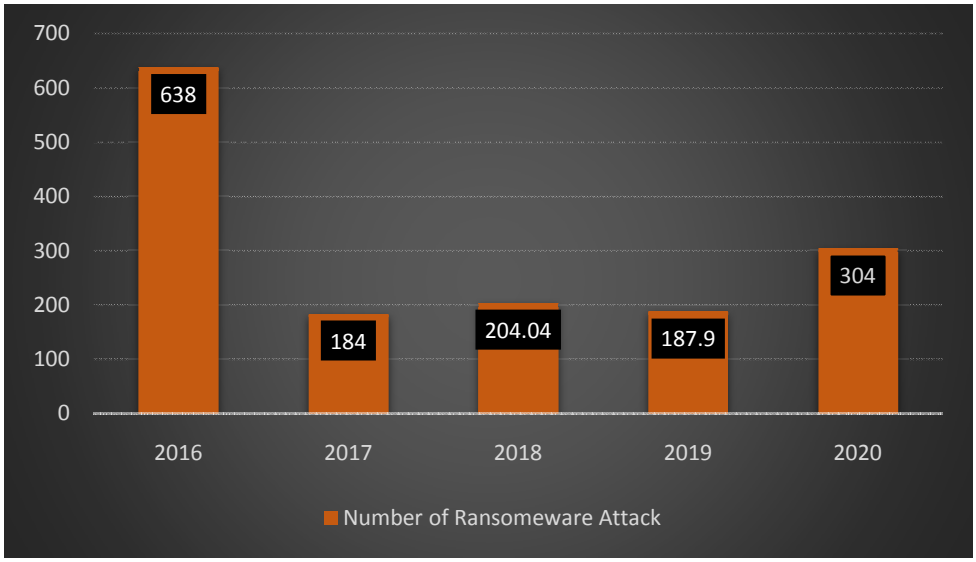

Figure 3: Annual Global Malware Infection Rate from 2016 to 2020.

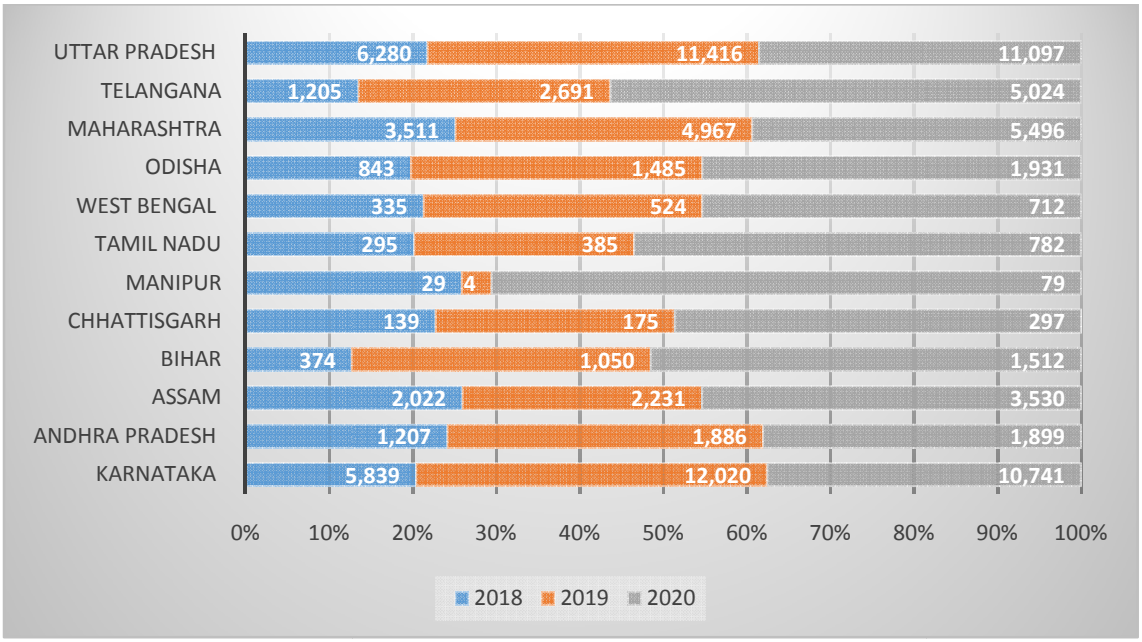

Figure 4: Depicts the Cybercrime Data in India Are Broken Down By State.

In the year 2020, the most incidences of cybercrime were reported in the state of Uttar Pradesh, with 11,097, followed by Karnataka, with 10,741 incidents. According to the data, Maharashtra came in second place with 5,496 cases, followed by Telangana with 5,024 cases in third place. The number of incidents of cybercrime in the following states increased significantly between the years 2019 and 2020: Telangana, along with the states of Arunachal Pradesh (from 7 to 30), Assam (2,231 to 3,530), Chhattisgarh (175 to 297), Goa (15 to 40), Gujarat (784 to 1,283), Manipur (4 to 79), and Gujarat (784 to 1,283) (2,691 to 5,024) shown in Figure 4. India is making great steps in the realm of technology, but the country also faces increasing problems with cybercrime. The purpose of the National Cyber Security Policy 2013 is to protect data and increase national defenses against cyber assaults. The overall goal of the strategy is to safeguard India's economic and strategic interests. The National Cyber Security Policy 2013 has 14 goals, some of which are: creating a cyber-ecosystem in the country; offering financial benefits to businesses for adopting standard security practices and processes; building effective public-private partnerships; engaging in collaborative engagements through technical and operational cooperation; and so on.

It is necessary to develop a strategy for the prevention of crime that includes well-defined priorities and objectives. Additionally, the government should incorporate long-term guidelines into the programs and structures it has in place to control crime, and it should make certain that the government has well-defined responsibilities and objectives for the organization of crime prevention. Legislation must take into account, in addition to the regulations that have traditionally existed, new ideas and things that are connected to computer data. To successfully prevent and fight cybercrime, it is essential to implement criminalization, procedural powers, jurisdiction, international collaboration, as well as duty and liability for internet service providers. Investigative procedures, legal jurisdiction, digital evidence, and international collaboration are all ways that help may be provided in this area, and it is very much required.

However, many small and medium-sized businesses mistakenly believe they will not be a target and do not take enough effort to safeguard their systems. The private sector is better aware of the cybercrime risk assessment and employs cyber-security technologies. Some

businesses, including the use of legal action, have already taken preventative measures to combat the acts of cybercrime that have been committed. Internet service providers and hosting providers have the potential to play an important part in the prevention of cybercrime. They could keep records that can be used to investigate criminal activities, assist clients in identifying systems that have been hacked, restrict certain types of unlawful information like spam, and generally maintain a secure communications environment for their consumers. Academic institutions are important partners in the fight against cybercrime because of their role in the generation and dissemination of new information, the drafting of new laws and policies, the creation of new technological and regulatory standards, the provision of assistance in the form of technical assistance, and their collaboration with law enforcement agencies. Everyone who uses the internet and conducts online transactions must take basic safeguards.

1. *Internet Security Suite:*

One may use anti-malware software, which is purchasable either online or offline, to safeguard or protect their information against various infections.

2. *Strong Password:*

Passwords should be strong and changed regularly. Passwords should be changed regularly using a mix of letters, numbers, and special characters, and an attempt to clear browser history after work is over, especially if using public or shared computers or laptops.

3. *Regular updating of the software:*

Criminals employ vulnerabilities and holes in operating systems and the internet to obtain access to systems, therefore maintaining regularly updated software is crucial for preventing cybercrime.

4. *Managing social media Settings:*

It is always critical to keep personal and private information secure. Cyber thieves monitor social media information; thus, it must be protected and passwords changed regularly. Share as little information as possible on social media so that no one can predict the answers to security questions.

5. *Intensify Home Network*:

Increase the Strength of Your Home Network- Your home network should have a strongly encrypted password and a virtual private network. A VPN is an abbreviation for Virtual Private Network, which enables you to establish a secure connection to another network through the Internet. It enables you to connect to public networks more securely. It's a good idea to use VPNs in both public and private networks to ensure protection everywhere.

6. *Secure Personal Computer and Mobile Devices:*

This may be accomplished by activating the computer firewall, using anti-virus and malware software, and preventing spyware assaults by constantly installing and upgrading software. In two-factor authentication, mobile devices must be updated and password secured, and software must be downloaded from a trustworthy source.

4. CONCLUSION

Cybercrime presents a serious threat to the personal safety of an individual and the national security of a country. Large-scale monetary effects are done to both private citizens and

businesses, although military technology is also put at risk. Millions of individuals are affected by big data thefts. The major goal of the study was to give insight into the progression of the dominance of cybercrime cases throughout India. This study indicates that several sorts of cybercrime are prevalent in this technologically advanced age. It has been determined that the number of cybercrime cases in various Indian states and cities has steadily increased over the last decade. The number of people apprehended in cybercrime cases recorded is very low. As a result, it is evident that our cyber frameworks and Indian cyber laws still have some challenges to sort out, as our Information Technology Act is incapable of providing total safety to our cyber world. As a result, appropriate execution of cyber laws, as well as awareness and correct policy formulation, are required.

REFERENCES

[1] A. M. Bossler and T. Berenblum, "Introduction: new directions in cybercrime research," *J. Crime Justice*, vol. 42, no. 5, pp. 495–499, Oct. 2019, doi: 10.1080/0735648X.2019.1692426.

[2] M. Imran, "Emerging Trends in Cyber Crimes in India: An Over View," *SSRN Electron. J.*, 2016, doi: 10.2139/ssrn.2818402.

[3] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[4] S. Varshney, D. Munjal, I. Jash, O. Bhattacharya, and S. Saboo, "Cyber Crime Awareness and Corresponding Countermeasures," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3601807.

[5] D. Thomas and B. D. Loader, "Introduction: Cybercrime: Law enforcement, security and surveillance in the information age," *Cybercrime: Security and Surveillance in the Information Age*. 2013.

[6] K. Dashora and P. P. Patel, "Cyber Crime in the Society: Problems and Preventions," *J. Altern. Perspect. Soc. Sci.*, 2011.

[7] S. Yu, "Fear of cyber crime among college students in the United States: An exploratory study," *Int. J. Cyber Criminol.*, 2014.

[8] S. Furnell and S. Dowling, "Cyber crime: a portrait of the landscape," *J. Criminol. Res. Policy Pract.*, vol. 5, no. 1, pp. 13–26, Feb. 2019, doi: 10.1108/JCRPP-07-2018-0021.

[9] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, p. 102248, Jun. 2021, doi: 10.1016/j.cose.2021.102248.

[10] J. Choi, B. Dulisse, R. L. Wentling, and N. Kruis, "Editorial introduction to the special issue: Supporting future scholarship on cybercrime," *Int. J. Cybersecurity Intell. Cybercrime*, vol. 4, no. 2, pp. 1–3, Aug. 2021, doi: 10.52306/04020121YRSY7883.

[11] K. Seth, "IT Act 2000 vs 2008-Implementation, Challenges, and the Role of Adjudicating Officers," *Natl. Semin. Enforc. Cyberlaw*, 2010.

[12] H. Saini, Y. S. Rao, and T. C. Panda, "Cyber-Crimes and their Impacts□: A Review," *Int. J. Eng. Res. Appl.*, 2012.

[13] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, and G. Saldamli, "Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure IoT layered Model," in *2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)*, IEEE, Oct. 2020, pp. 113–118. doi: 10.1109/MCNA50957.2020.9264301.

[14] H. Zolfi, H. Ghorbani, and M. H. Ahmadzadegan, "Investigation and classification of cyber-crimes through IDS and SVM algorithm," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE, Dec. 2019, pp. 180–187. doi: 10.1109/I-SMAC47947.2019.9032536.

[15] S. Batra, M. Gupta, J. Singh, D. Srivastava, and I. Aggarwal, "An empirical study of cybercrime and its preventions," in *PDGC 2020 - 2020 6th International Conference on Parallel, Distributed and Grid Computing*, 2020. doi: 10.1109/PDGC50313.2020.9315785.

[16] P. Datta, S. N. Panda, S. Tanwar, and R. K. Kaushal, "A Technical Review Report on Cyber Crimes in India," in *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, IEEE, Mar. 2020, pp. 269–275. doi: 10.1109/ESCI48226.2020.9167567.

CHAPTER 12

RELEVANCE OF ISLAMIC LAW IN FORMULATING BUSINESS LAW

Ms. Razina Ahmed, Assistant Professor,
School of Law, Presidency University, Bangalore, India,
Email Id-razina.ahmed@presidencyuniversity.in

ABSTRACT:

Cited entrepreneurship as the main driver of national economic growth and as a catalyst for it. Islam constantly urges its adherents to become involved in the business right away. Muslims will be inspired to succeed as an entrepreneur in this world and the hereafter if they see their work as a kind of religion. However, there are Muslim business people that operate their enterprises whether they are legal or illegal from an Islamic perspective. They engage in unethical (bad) commercial practices to generate profit. Islam's view of business ethics may help someone become a responsible businessperson. Fearful business people will never waver in their commitment to achieving their goals fully and following Islamic law. To maintain high ethical standards among entrepreneurs, every businessperson should consistently follow Islam based on the Quran and the Sunnah and be resourceful, fair, honest, trustworthy, and genuine in all business establishments.

KEYWORDS:

Business, Islam, Entrepreneurship, Lawful, Unlawful.

INTRODUCTION

The Qur'an and the Sunnah are the foundational texts of Islamic law. It is sometimes referred to as the union of two significant sources of Islamic law that connect revelation and reason. The most revered book in the world, the Quran, has passages that discuss human views and morality. The Sunnah, a collection of sayings from the Prophet Muhammad, is the second source. Both the Quran and the Sunnah include a wealth of legal information. Additionally, according to the sources, the Church will never accept two contradictory interpretations. The texts also include explanations of the rationale behind Islamic law-making. In Islam, the law is legitimate and able to tackle every criminal situation, regardless of the time or location. It also calls for legal reasoning, which results in a different body of law known as legal reasoning. Instead of causing disparities in traditions and beliefs, it produces the same effect without interpreting the language of the other two sources. The sources contain several legal decisions that have left room for judicial interpretation.

Where Islamic law originated Sharia lays down the laws and guidelines that govern a Muslim nation and establishes a bond between God and all people, Muslim or not. The Hadith and Sunnah are complementary, equal sources for the Quran (Janin and Kehlmeyer, 2015). There are ethical rules that have been endorsed, advised against, outlawed, and sanctioned. The Sharia encourages Islamic people to get involved in business activities. where Islamic law originated Sharia lays down the laws and guidelines that govern a Muslim nation and establishes a bond between God and all people, Muslim or not. The Hadith and Sunnah are

complementary, equal sources for the Quran (Janin and Kehlmeyer, 2015). There are ethical rules that have been endorsed, advised against, outlawed, and sanctioned.

There are numerous categories in Islamic Finance, including:[1]

1. Murabaha.
2. Ijara.
3. Musharaka.
4. Ijara-wa-Iqtina.
5. Mudaraba.

These values have their roots in the trusteeship's foundation of accountability and faith in Allah's devotion. Hard work and productivity are valued and rewarded. Business morals are a bunch of concepts and rules that should be kept while directing business, simply deciding, and managing others overall. Islamic regulation is significantly not the same as Western regulation and depends on transactions. Individuals in the Islamic business world experience issues concerning adhering to the law and drafting gets that follow Islamic regulations. There are a few investigations of business in Islam that give data on both the public great and how trade is permitted under Islamic regulation. The laws of Sariah, the foundation of Islam, are utilized to determine questions when they emerge, and the dialects used to do so are Bosnian and English writing (Ahmed, 2018). With regards to keeping funds altogether and involving them as an instrument for public requesting, there is likewise a lawful plan. The market incorporates contracts for money, banking, and numerous different businesses, as per the web-based task help administration. The utilization of chance sharing and speculative exchanges is similarly denied in Islamic banking. It has no different codes save Sharia, which the administrative power has endorsed. By "authoritative power," we mean the power of a firm, which has its standards and guidelines.

The management goals are

1. The following system has structures and procedures.
2. Maintaining values with policies, objectives, ethics, and strategies.

Islamic entrepreneurship [2]

1. Risk-taking is prohibited in Islam.
2. Satisfying obligations that are related to religions.
3. Working with productive firms.

Islam's veritable business reasoning underscores opportunity, respect for others' necessities, and equity for the individuals who maintain the law and are devoted to the regulations that are expected to be followed come what may.Saudi Arabia is the nearest to having an Islamic state among the few Islamic countries. Furthermore, the country is empowering monetary endeavors and establishing regulations to help and advance worldwide speculations. In Malaysia and Egypt, there are Islamic courts that assist with peopling resolve their legitimate debates as per Islamic regulation. Indeed, even unique assessments and corporate standards should be continued to support collaborations with outsiders. The Sharia can't be modified just to oblige the contemporary goals of different countries. These guidelines are intended to maintain equity between market purchasers and dealers. Islam has business-related guidelines that incorporate things like keeping restricted associations.

Principles of Islamic Business Ethics[3]

Standards of Business Ethics in Islam In the Quran there are around 370 sections that show us, particularly Muslims, the method for working with an ethical balance, alongside a client that restricts us from committing specific errors (Hakim, 2012: 202). Notwithstanding the investigation of business morals because of the Qur'an. The illustrations from business morals itself can be drawn from the way of behaving or the day-to-day existence of the Prophet Muhammad because the Sunnah is likewise a wellspring of regulation in Islam other than the Qur'an. Muhammad in the verifiable survey is known as an exceptionally effective financial specialist, so in business, morals concentrate on it is extremely important to check out Muhammad's business conduct during his lifetime. Muhammad's dedicated mindset was framed from their youth when he was raised by Halimah Assa'diyah to adulthood. Muhammad, who was 4 years of age, was grouping goats alongside Halimah's youngsters. This experience was subsequently utilized as crafted by grouping goats having a place with the occupants of Makkah (Muhammad, Saifullah, 2011: 216). Here are a few moral rules in business/business that have been exemplified by the Prophet Muhammad Saw (Abdul. Aziz, 2013: 31):

a. Honesty is the most necessity in business exercises. At this level, he said "It isn't passable for a Muslim to sell a deal that has shame, except if he makes sense of his shame," (H.R. Al-Quzwani). "Who hoodwinks us isn't our gathering" (H.R. Muslim). The Prophet himself is an illustration of conduct that is continuously telling the truth in business. He precluded brokers from putting spoiled merchandise at the base and new products at the top. Trustworthiness applied by the Prophet is the epitome of the customer-arranged guideline in the ongoing setting, in particular the business rule that generally keeps up with consumer loyalty (Afzalur Rahman, 1996). The effect of the standards applied by the Prophet Muhammad SAW, the clients of the Prophet Muhammad never felt hurt and there were no bad things to say about the commitments made, because the merchandise settled upon in the agreement were not controlled or diminished. With client situated providing shoppers with the decision of room for the option to pay (proceed or drop an exchange) on the off chance that there means misrepresentation or the buyer feels distraught (Muslich, 2010). This Khiyar idea can be a calculation fortifying the place of shoppers according to makers, with the goal that makers don't act randomly towards their clients.

b. Help or benefit others, a consciousness of the social meaning of business exercises. In Islam, the money manager doesn't just seek after benefit, as shown in the Capitalist Economy, but at the same time is situated towards ta'awun (helping other people) as the social ramifications of business exercises.

c. No cheating. The estimation sizes and scales should be right. The Word of God: "Hardship to the people who cheat, the individuals who, when they get an action from another person, they request to be satisfied, and when they measure or weigh for other people, they decrease" (QS 83: 112). A finance manager or maker is expected to have a straightforward nature. The Straightforwardness of this record is the point at which a maker can apply transparently to quality, amount, creation, and others.

d. You can't attack others' organizations, so individuals get them. The Prophet Muhammad said, "Let not one of you sell fully intent on criticizing what is sold by another person," (H.R. Muttafaq 'Alayhi). Islam regards business rivalry, however, rivalry should not legitimize any means, since it is in opposition to the standards of muamalah in Islam. Islam approaches followers to continuously contend in goodness, not to thump each other down. Rasulullah has given instances of how to contend well and deny out-of-line rivalry. As referenced in QS. Al Baqarah refrain 188: And let not one of you eat the abundance of the other piece of you by vanity and (don't) carry the make a difference to the adjudicator, so you might eat a portion of the property of others with (the approach to doing)) sin, even though you know.
e. Do not crowd merchandise. In Islam, this term is called Ihtikar. Ihtikar is storing products (stacking up and putting away merchandise inside a specific period, with the point that the cost will ultimately rise and an enormous benefit is gotten). This act is denied by the Prophet.
f. Do not do a restraining infrastructure. Syndication is completely disallowed in Islam. Islam doesn't approve of the abuse (control) of specific people of social property privileges, for example, water, air, and land and their items like minerals and minerals.
g. Selling just halal business products are not unlawful merchandise, like pigs, canines, alcohol, happiness, etc. The Prophet Muhammad said, "Verily Allah precludes the matter of liquor, corpses, pigs, and sculptures," (H.R. Jabir). In the current setting, Muslims are likewise frequently caught not to drink pork. These two sorts of items don't unequivocally become Muslim utilization or product, yet the subordinate results of these two items are generally coursed and, surprisingly, exchanged by the Muslim people group.
h. Business should be liberated from usury. The Word of God, "O you who accept, leave the leftovers of usury assuming that you accept," (Surat al-Baqarah: 278). Entertainers and eaters of usury are considered by Allah as steadfast individuals (QS. 2: 275). Consequently, Allah and His Messenger proclaimed battle on usury.
i. Business is done willfully, without compulsion. The Word of God, "O you who accept, don't eat your neighbor's property in a vanity way, besides in the method of business that wins and likes you," (Qur'an 4: 29).
j. Paying compensation before workers sweat dry. The Prophet Muhammad said, "Give wages to the representatives before the perspiration dries." This hadith shows that the installment of wages should be rushed and ought not to be deferred. What's more, one of the commitments of managers is to give fair wages to representatives, not exploit and safeguard the freedoms of workers [4].

Islamic Law of Business Organization

Either a contract or the blending of resources might result in a partnership. Due to this, the forms of partnerships have been categorized by jurists into three categories: sharikat al-ibahah (common sharing of goods), sharikat al-milk (co-ownership), and sharikat al-aqd (partnership by contract). We searched the scholarly literature for a definition of partnership that encompasses all three forms but were unable. According to Abd al-Aziz al-Khayyat, this is due to the disparity in the terms and regulations governing the various kinds of partnerships. Al Kayyat believes that the diversity in the guidelines and requirements for the various kinds of partnerships is the solution to this problem. Al-Khayyat attempts to provide a universal definition by expanding on the Hanafi definition, which defines shariah as "the exclusive right of two or more individuals to a single subjectmatter," to get over this problem.

When it comes to the appropriateness of this concept as a broad definition, we would want to disagree with al Khayyat. The definition of sharikah in the meaning of the partnership contract or even a generic term has been provided in the Majallat al-Ahkam Al-Adliyah. He uses a generic term and the Hanabali definition within it.

Shari'a Commercial Law in the Modern World [5]

However, there are some practical problems. Since the Shari'a commercial system was dismantled many years ago, we cannot be entirely sure what the shari'a way is, nor how it was practiced. We have texts written by the jurists, but controversy surrounds the issue of the degree to which they reflect the law in action; our best source of information, the participants in the system, died many years ago; records relevant to practice are sparse for most periods, and where they do exist only a few of them have been researched.[6] An example of the controversies can be seen in the differing conclusions drawn by two eminent scholars, Emile Tyan, and Abraham Udovitch. Tyan concluded from a study of notarial documents that the Hanafi rules on hawala (the transfer of a right or obligation) were significantly different from the law in action.[7] Udovitch, on the other hand, after studying the Cairo Geniza documents, wrote: 'There is an almost one-to-one relationship between the importance of problems as reflected in the Geniza papers, and the amount of space and attention they receive in the law books', and: 'Hanafi commercial law, especially that portion of it dealing with institutions of commercial association, had a very close relationship to actual practice'.[8] Perhaps both were right as regards the documents they studied in the context of their time and place. As Mallat observes, 'the exact interaction between law and reality in the classical age has not been tested in any significant manner'.[9]

However, this difficulty may be less problematic than it seems. Without going into the complexities of the debate, we can probably say with some assurance that, in many places and for long periods in most areas of commerce, the law in the books mostly reflected the law in action.[10] Hanna's extensive study of court records, for example, clearly demonstrates that commercial law played a vital part in the daily professional life of merchants in the Egypt at that time.[11]

The Concept of RIBA

Most financial specialists associated with the Middle East know that Shari'a regulation precludes interest in advances. This, nonetheless, is only one use of the more extensive idea of "riba." Although an exact and generally acknowledged definition is subtle, riba fundamentally implies unmerited or ridiculous benefit. Riba is censured on the ground that getting something in return for no good reason is unethical. [12] Profit acquired from theoretical exchanges is censured as riba. Betting falls into this classification, however, the idea that gamble (gharar) is off-base is reached out to forbid any exchange wherein the addition of each party isn't characterized at the time the agreement is made. By Shari'a principles, numerous advanced business exchanges contain components of riba or gharar. To keep away from riba, a vendor should effectively add esteem before he exchanges the item. For instance, a tenant couldn't sublease property for more than he is paying the proprietor because the benefit would be unmerited.

Similarly, a vendor must essentially claim property before he exchanges it, any other way he could never have added any worth. Any agreement that left the installment term open either the sum or the date due [13] or attached it to some standard that varies, for example, the market cost or the great pace of revenue, would be void since it included gharar. For instance, if the cost term was expressed as the predominant market cost of an item at a point from here on out, the gatherings would bet; an enormous swing in cost for sure would create a bonus for

one party. Any agreement where a commitment is contingent on the event of an occasion that probably won't happen, for example, an insurance policy would likewise imply risk or gharar and subsequently be void [14]. An outrageous model is that a development contract that determines both the task to be finished and a consummation date could be void because of the gamble that unexpected conditions could emerge that would keep the project worker from satisfying the agreement.

The undeniably enforceable and generally liked type of agreement in Shari'a is an offer of products with the unrestricted and prompt exchange of responsibility for existing items in return at a decent cost. This exchange disposes of any gamble that one party could create an unanticipated gain out of the exchange. For such a deal to be substantial, the move of possession should pass quickly upon the finish of the agreement; assuming the exchange of proprietorship is passed on to the future, a component of the hypothesis is presented that sounds unsatisfactory.

Contracts for the offer of merchandise to be produced are perceived, however, are revocable by one or the other party preceding the fruition of the assembling system. [15] Service or recruit contracts should definitively characterize the sort of administrations to be played out, the thought (wages or lease), and the time of recruit.' Specific exemptions for these standards exist for certain kinds of exceptional exchanges. For instance, two gatherings can begin a business in which one furnishes capital and the other work with consent to separate the benefits. This is known as a "mudaraba," ' and is substantial even though the remuneration and measure of work is dubious. The outcome of going into an agreement that is spoiled by Riba is that the courts won't implement it.

The courts will, nonetheless, use the precedent-based regulation's idea of even-handed solutions for re-establish the gatherings to the places that they had before going into the agreement. One who got administration would need to pay for the worth got. A purchaser who had the utilization of a house in a deals exchange that is void would pay the vendor lease for the time of inheritance.'

Recession

On a few occasions,Sharia regulation permits the gatherings to revoke in any case substantial agreements. The option to cancel emerges in the circumstance in which the dealer has not performed. The purchaser might cancel the agreement assuming an imperfection exists in the merchandise that significantly weakens the worth of the products. In a help contract, the purchaser can disavow on the off chance that the nature of administration isn't a guarantee of merchantability. Dissimilar to the custom-based regulation, this option to repudiate can't be postponed or avoided by contract, and the merchant weights demonstrating the shortfall of any deformity. In agreements that include a continuous relationship, like office, association, permit, or the stockpile of labor and products on a proceeding with the premise, each party has the privilege to end the agreement singularly whenever regardless of whether the agreement determines a time of term.

In an agreement that includes a continuous relationship, such as an official association, permit, or the stock of labor and products on a proceeding with the premise, each party has the privilege to end the agreement singularly whenever regardless of whether the agreement determines a time of term. The courts might require the ending party to make some even-handed compensation for the other party's prompt misfortunes, however, they are probably not going to make him entirely by Western principles. This is because Shari'a doesn't perceive the idea of considerable harm. Computation of harms by Shari'a courts never considers expected benefits since that is a questionable matter.

Conditions in the Contract

Agreements in an agreement characterizing the merchandise to be conveyed, the administrations to be performed, or the strategy and measure of installment, are seen by Shari'a as legitimate and vital. Conditions in an agreement that is "despite the pith of the agreement," in any case, are viewed as void under Shari'a. A model would be a condition in an offer of products that would restrict the purchaser's opportunity to utilize the merchandise, like prohibiting him to exchange them for someone else. Hence, conditions in a permit of innovation that force regional limits or secrecy commitments may not be enforceable. A third classification of conditions comprises terms that are viewed by Shari'a as irrelevant to the embodiment of the agreement. Whether these irrelevant circumstances will be implemented relies on whether they are viewed as significant or non-significant. The accompanying models help to outline significant and non-significant circumstances: "Merchant offers his camel to Buyer on condition that Seller is permitted to ride it back to his home." X leases his home to Y on condition that X loans him an amount of cash. "Purchaser purchases a piece of fabric on condition that Seller tailors it. The principal model is viewed by Shari'a as a minor or non-significant condition. The second and third models are significant circumstances that Shari'a would treat as void except if separate costs are expressed for each condition. The reasoning is by all accounts that assuming more than one autonomous exchange is involved, the gatherings ought to enter separate agreements; in any case, a vulnerability exists concerning how to distribute the thought between the two particular arrangements.

Implementation Of Islamic Business Ethics [16]

Islam offers various options for implementing business ethics. One of them is that a trader or businessperson needs to be familiar with Islam's rules and business ethics. They must read and comprehend the concepts contained in the Qur'an and Sunnah. They must also have faith that they will face Allah on the Day of Judgment, which will make them fear disobeying Him. They should therefore adhere to and follow the business ethics that Islam has approved. Without this trust, entrepreneurs may start to try to avoid conducting business following Islamic ethics, particularly when it requires expense, effort, and time. Additionally, users should be aware of Islamic business ethics and verify that merchants or business owners adhere to them. To discover that there are a few business owners who engaged in fraud or violated the defined standards of business ethics, they should be actively involved in defending the rights of the users and report the information to government agencies and the private sector. The government also has a crucial role in ensuring that firms and entrepreneurs understand and follow the requirements by distributing detailed instructions and comprehensive information on Islamic business ethics. To oversee the application of the rules equitably, unbiasedly, and without partiality, a government agency or organization should be established. It should also give people a place to voice their complaints and share information if there are any inconsistencies.

CONCLUSION

Business isn't just a wellspring of a living even be one of the parts of confidence that can move nearer to Allah. Making business a type of love will urge a Muslim to become business people who are devoted to God and find lasting success in the organizations. As per Ab, (2009), the outcome of the pioneering exercises of Islam relies upon the blend of discernment and solid collaboration between the three gatherings, the church, mark, and business visionaries themselves. Every one of the three of these individuals needs to assume their separate parts that meet up with one another and subsequently can fulfill the needs of a relationship with Allah (habluminanallah) and guarantee to keep human relations

(hablumminannas). Consistency is viewed as one of dedication that will be compensated concerning material blessings or prizes from Allah. This implies that the idea of business venture in the Muslim world over for benefit goals as it were. In this way, understanding the business as mandatory kifayah empower Muslims particularly for graduates to become business people or merchants that can give the requirements of different Muslims, and hence have the option to foster the financial matters development of a country. Hence, the individuals from an association ought to be driven by a total arrangement of morals with regard to a complete Islamic structure. The presence of an equal framework, the association of work practices, and the conduct of individuals in an association given Islamic regulation cases would work with the acknowledgment of true Al-Falah in the administration and organization of an association.

REFERENCES

[1] "Discuss The Relevance Of Islamic Law In Formulating Business Law." https://omanessay.com/the-relevance-of-islamic-law-in-formulating-business-law/

[2] M. A. Ashraf, "Theory of islamic entrepreneurship: A conceptual paper," *Int. J. Entrep.*, 2019.

[3] "Some Key Business Ethics Principles in Islam", [Online]. Available: https://theislamicworkplace.com/2009/03/03/some-key-business-ethics-principles-in-islam/

[4] "Ma'amor, O. (2001). Business ethics: Islamic perspective. Malaysia: Prentice Hall.".

[5] "On the 'restoration' issue generally, see HALLAQ, WB (2004) 'Can the Sharia Be Restored?' in HADDAD, YY and S TOWASSER, BF (eds) Islamic Law and the Challenges of Modernity AltaMira Press.".

[6] "RAY, ND (1997), pp.47-49.".

[7] "TYAN, E (1946), pp.31-37. Views such as this are considered by some scholars to be a means of 'relegat[ing] Islamic law to the status of a relic of the past' to make it seem 'archaic, rigid, primitive, and incapable of change', enabling colonial adminstra".

[8] "Udovitch, AL (1970B), p. 290.".

[9] "MALLAT, C (2003), p. 735.".

[10] "RAY (1997), p. 45".

[11] "HANNA, N (1998)".

[12] "N. COULSON, supra note 1, at 11".

[13] "N. COULSON, supra note I, at 20; A. Doi, SHARI'AH: THE ISLAMIC LAW 381 (1984); Hill & Abbas, Comparative Survey of the Islamic Law and the Common Law Relating to the Sale of Goods, 2 J. ISLAMIC & COMP. L. 88, 98 (1968).".

[14] "N. COULSON, supra note I, at 44. The sale of animals unborn or fish not yet caught or agricultural products not yet harvested are all forbidden.".

[15] "N. COULSON, supra note 1, at 21.".

[16] I. H. Ismail and M. Nur, "Implementation of Islamic Business Ethics as a Competitive Strategy at PT Mahesa Energi Persada Jakarta," *JUDICIOUS*, 2021, doi: 10.37010/jdc.v2i2.484.

CHAPTER 13

A COMPREHENSIVE STUDY ON CONSTITUTIONALISM AND ITS IMPACT ON DEMOCRACY

Mr. Ranjeet Mathew Jacob, Assistant Professor,
School of Law, Presidency University, Bangalore, India,
Email Id-ranjeet.mathew@presidencyuniversity.in

ABSTRACT:

The concept of constitutionalism emphasizes that where governments are necessary, their powers be legally restricted and the legitimacy of the administration rests on respecting these restrictions. Uniform democracy causes disintegration because leaders are always changing, which gives rise to corruption, democratic competition, and power dramas are the only things that leave no room for morality. Hence in this paper, the author focuses on the principles of constitutionalism which provide for law and order, division of powers, commitment to responsible governance, popular sovereignty, fair judiciary, and rule of law. Also discusses the effects of constitutionalism on democracy such as public reason in political constitutionalism in a democracy and a comparison of political and legal constitutionalism. It concluded that the unfortunate fact of the Indian administration is a political and administrative offense, and this cancer has to be removed immediately from the system of Indian democracy. In the future, the rule of law is guaranteed by constitutionalism, which is widely regarded as essential to democracy everywhere.

KEYWORDS:

Constitutionalism, Democracy, Government, Law, Political.

1. INTRODUCTION

Constitutionalism is the idea that a country's legal system or its constitution determines the power of its government. Even while constitutionalism is occasionally seen as a shorthand for smaller governments, this view is only one but by no means the most well-known in the past. Constitutionalism more broadly refers to efforts to stop arbitrary governance. The capacity of rulers to govern willingly, with complete discretion, and to further their interests instead of those of the ruled is referred to as arbitrary nature at its most generic level. By creating systems that limit who may rule, how they can rule, and for what objectives, constitutionalism seeks to avoid these dangers. On what constitutes arbitrary conduct, nevertheless, and which safeguards work best against them, constitutional conventions diverge [1],[2]. By producing a condition of political equality marked by a power balance between all relevant groups and organizations, the classical republican tradition, as interpreted by its Neo-Republican interpretation, links political constitutionalism to dominance governed by its rulers. So that no one may dominate within a polity without considering the interests of the ruling. The more contemporary, liberal tradition views

arbitrariness as an infringement on individual rights and works to defend those rights by establishing a division of powers and a legally binding constitution.

The process of creating a constitution may involve several collective groups, including legislative bodies, executive bodies, circular tables, political conventions, and component conventions. But in democracies, the last two seem to be the most typical instances of legislatures that serve as forums for debate, negotiation, and ultimately voting on constitutional provisions. As a result, it will limit my research to the constituent convention and assemblies, comparing their character, frequency, their organizational structure to one another [3],[4]. Constituent assemblies are gatherings established with the specific aim of proposing or introducing a new constitution. This definition identifies the essential characteristic of these organizations as the requirement that they are dissolved upon the adoption of the new constitutional text. Though conventions could also be used to approve or put forth revisions to an existing constitution, they will only concentrate on their basic purposes in this article. Finally, while there are other ways to elect convention delegates, it will concentrate mostly on elected conventions since popular elections are by far the most typical method for choosing all constituent assembly since at least the nineteenth century. In the process of establishing democratic republic and democratic governance, in particular but not only.

In a representational government, citizens choose representatives to cast ballots and carry out other political duties on their behalf. Therefore, direct democracy, in which every legislation or policy being considered at every level of government is decided by popular vote, is the antithesis of representative democracy. Typically, representative democracies are used in large nations when direct democracies would be impossible to operate with so many persons participating. A constitution that provides the fundamental rules, values, and structure of government defines the powers of elected representatives [5],[6]. The constitution may also allow for various types of restricted direct democracy, such as in addition to calling elections and removing votes, elected officials may have the authority to choose the president or chancellor from among independent judicial bodies, such as the American government. The Supreme Court may have the authority to deem representatively constituted laws to be unconstitutional.

1.1. History of Constitutionalism and Democracy:

A constitution that provides the fundamental rules, values, and structure of government defines the powers of elected representatives. The constitution may also allow for various types of restricted direct democracy, such as in addition to calling elections and removing votes, elected officials may have the authority to choose the president or chancellor from among independent judicial bodies, such as the American government. The Supreme Court may have the authority to deem representatively constituted laws to be unconstitutional. However, since one cannot control oneself except, in a metaphorical sense, Austin and Hobbes argue that the concept of the limited sovereign is incompatible with the concept of a square circle. Austin claims that any group or individual with unrestricted power can claim sovereignty on behalf of the people. Constitutional law may place restrictions on some government entities, such as the parliament or the court, but the people's sovereignty is unrestricted. However, we have if we associate the leaders with the populace. Hart, the commander issuing instructions to the commanders, has detected inconsistent results.

The present paper is a study of a democratically elected government that is given legitimacy through the idea of constitutionalism. This should not be confused with the validity of the actions taken by government authorities, and neither should it be. The importance of

constitutionalism outweighs the value of a written constitution. This study is divided into several sections, the first of which is an introduction, followed by a review of the literature and suggestions based on previous research. The next section is the discussion and the last section is the conclusion of this paper which is declared and gives the result as well as the future scope.

2. LITERATURE REVIEW

H. Kumar and S. Godara have explained that Even though constitutionalism opposes authoritarian authority, the government must play a transparent and ethical role that respects the rights of citizens. The fulfillment of several basic rights and the current effectiveness of the implementation of those provisions in courts are the major goals of the study. According to the author, since constitutionalism has been implemented in many countries, individuals now have the freedom to speak freely, challenge government decisions, elect a national government, and exercise other political and military rights. It was found that the extent of Fundamental Rights has increased considerably as a result of the realization that these rights must be protected with time. It was concluded that constitutional law has facilitated social change in most of the countries of the world including India.

Verena Frick [7] has explained using historiography on German constitutionalism after 1949 as a starting point. It examines how law and politics interact within German constitutional thought by tracing its origins and development through scholarly discussions. The author has reconstructed a significant change in the meaning of the word constitution, showing how it moved from a somewhat formal and ad hoc means of governance to a fair value system of politics. The paper pointed to a fundamental change in the meaning of the Constitution, from being merely an instrument of administration to a declaration of a fair value order of politics. It concluded that implementing the program of constitutional equality under the watchful eye of a powerful custodian of the Constitution is accomplished through democratic politics.

Imran Ahmed [8] has explained that the role of constitutional courts is still a matter of debate, and experts differ on the democratic credentials of judicial review, which also largely ignores the function of the Islamic court system. The author says that three recent studies focused their attention on Pakistan in these discussions. It was indicated that these three studies contributed significantly to the identification of significant obstacles to the judicial institution establishing its democratic credentials. It concluded that consensus on the scope and limits of judicial review is still necessary as the country faces uncertainty as long as the three organs of government continue to struggle and undermine the democratic system.

Olena Sihvo [9] has explained that To solve the complex situation of democracy in international law, where international lawyers have been forced to choose between two incredibly cautious strategies. The author claims to have created a contextual, context-aware approach to democracy, but within acceptable limits that would result in a scary legal discourse. It shows that the traditional liberal notions of state sovereignty, domestic jurisdiction, official consent, non-interference, and the territorial integrity foundation of legal positivism are no longer the foundation of international law. It concluded that foreign law recognized the authority of democratic government and established both internal and external means to uphold that authority.

Jernej Letnar Cernic [10] has explained that The legitimacy and credibility of every constitutional democracy depend on the strict adherence to its basic principles. The author examines conceptually how constitutionalism and militant democracy interact. The author claims to have studied the case law of the European Court of Human Rights concerning aggressive measures used to defend the idea of constitutional democracy. Consequently, the

Court's case law affirms that communal measures of militant democracy should be avoided and, wherever possible, replaced with individual measures. It concluded that barring the most serious instances, the European Court of Justice had exercised restraint in its case law regarding the banning of collective acts of extremist democracy such as political parties, associations, and election lists.

The above study shows that The role of constitutional courts is still a matter of debate, and experts differ on the democratic credentials of judicial review, which ignores the function of the Islamic court system as well as the legitimacy and credibility of each constitutional democracy as its core principles. In this study, the author discussed the impacts of Constitutional on democracy which depend on various factors are the development of democracy, democracy in the modern world, improving democracy, and democratic constitution-making bodies.

3. DISCUSSION

The government of the people, by the persons, and for the people is known as a constitutional republic and is founded on the primacy of the Constitution. Another way to put it is that it is a democratic system where the people's will is respected, their basic human rights are upheld, and the rule of law is firmly upheld. It is a type of democracy that the Constitution's provisions are established, ruled, and managed.

3.1. Principles of Constitutionalism:

The Constitution's restrictions are not restrictive in and of themselves. Mostly because the Constitution says so, dictators won't magically transform into kind leaders. To prevent a breach of the Constitution's language and spirit, there should have been a series of institutional mechanisms. Constitutionalism, according to Louis Henkin, is the development of the following components in Figure 1:

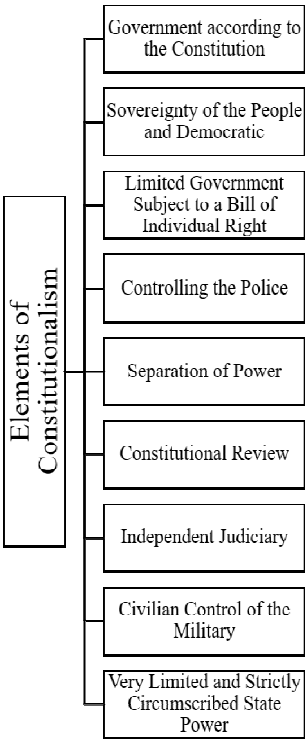

Figure 1: Illustratesthe Constitution's Elements Mandate that the Government has a Certain Set of Institutional Structures.

3.2. Development of Democracy:

Although there were likely definitely earlier examples of rudimentary democracy in other regions of the world, the ancient Greeks are attributed to being the first ones to form democracies. Around the city of Athens, in the fifth century BC, the Greek model was developed. Democracy stood out amid the sea of autocratic regimes and oligarchs that predominated at the time. Furthermore, the Athenian system had two key distinctions from how we currently view democracy: they practiced a sort of direct democracy, or, to put it another way, they chose to rule directly as opposed to electing representatives to do so. The fact that individuals were of a relatively narrow range made such an organization practicable. People convened, debated issues of government, and then put the decisions they had made into action. A tiny portion of the population was able to directly participate because women, slaves, foreigners, and youngsters were not allowed. Out of a community of around 400,000 males, there were still considerably more participants than in a modern democracy: these men were actively involved in politics.

3.3. Democracy in the Modern World:

As many different types of democracy exist now when there are democratic nations worldwide. One system cannot be used as a model for another since no two components are precisely comparable. There are parliamentary and presidential democracies, federal or unified democracies, majority-voting democracies, majority-proportional voting democracies, democratic countries that are also monarchical, etc. The use of political representatives is one aspect of contemporary democracies that unites them and distinguishes them from the historical model. Modern democracies employ elections to choose members who would be sent by the people to make decisions on their behalf instead of engaging in direct lawmaking. Democracy in this sense is referred to as representational. It can at least to some extent be said to be a democracy since it is built on the two aforementioned tenets of equality for all (one person, one vote) and the right to a certain measure of personal liberty for each person.

3.4. Improving Democracy:

Usually after free and transparent elections people often discuss how a nation becomes a democracy. However, democracy is much more than just elections, so when we are trying to assess it, it makes more sense to focus on popular will rather than institutional or voting systems. Because people can always have more, not something that may or may not exist, democracy is easy to understand. Almost always, democratic institutions can be reformed so that they are more democratic, more reflective of people's preferences, and more receptive to their influence. In other words, the individual's share of democracy can be improved by involving more people in decisions, and the power or will element of democracy can be improved by providing more real rights to the people. The fight for democracy has often focused on one or the other of these aspects whether through history.

3.5. Public Reason for Political Constitutionalism in a Democracy:

A complete, though brief, assessment of public causes forms the basis of the political formulation of constitutionalism. This idea includes both majority rule and equal votes. When viewed in this light, public cause enshrines the two most valuable democratic ideals: accountability and racial rights. This basic knowledge of the common good should be left open to public discourse so that other perspectives can be incorporated and new topics can be created for debate [16]. In other words, it accepts the trivial idea that public logic guides and controls public discourse, but it must also be based on that discourse. It enables obtaining or establishing difficulties that are considered part of the public cause, as well as the fact that

disagreement with the public objective is an expression of imagination and creativity and the correct idea of the imminent in politics. At this point, the legal definition and the political definition of a public cause differ significantly. There are pre-political features that legal true conservatives believe prevent public debate.

For example, fundamental rights are considered to be pre-political in origin and act as a check on the power of the majority. Consensus can be reached on certain topics after careful consideration and public discussion. Once a decision is made, there cannot be any more legitimate discussion on these matters. It is helpful to focus on Bellamy and Waldron's critique of Rawls' thesis in understanding the distinction between political and legal considerations of public cause. In Rawls' opinion, the public argument is confined to issues of fundamental objectivity and constitutional necessity. The conceptual background is a prerequisite for the formulation of Rawls' public arguments. Through this device, citizens, without a sense of justice, but with knowledge of their social and economic status as well as moral authority, chose two rational principles upon which two rational agents could agree. Since constitutional rules are designed to select only the most effective founding documents, the same basic principles will serve as an attempt to guide output causality because it is easier and more likely that individuals placed in the initial position are the same. Huh. Huh. Huh. Knowledge sharing will be the basis of justice.

3.6. Democratic Constitution-Making Bodies:

The process of creating a constitution may involve several collective groups, including legislative bodies, executive bodies, round tables, national conventions, and constituent conventions. However, in democracies, the last two serve as the most typical legislatures that debate, bargain, and ultimately vote on provisions of the Constitution. Since they differ in character, frequency, and management structure, I shall limit my research to representative conventions and legislature. Constituent assemblies are gatherings established with the specific aim of adopting or advancing a new constitution. This definition identifies the essential characteristic of these organizations as the requirement that they are dissolved upon the adoption of the new text of the constitution. Even though conventions may also be utilized to enact or put up constitutional modifications. Finally, even though delegates can be chosen in several ways, it will concentrate mostly on elected conventions since public elections seem to be the most typical means of choosing all constituent assemblies in Table 1 since at least the nineteenth century. In the process of establishing democracy and democratic government, in particular, but not only.

Table 1: Represent the Constitution-making bodies in a democratic government in which all based in Latin America were adopted by conventions [11].

S. No.	Country	Sub-Region	Year	Region	Legal	Constituent Body
1.	Denmark	Western	1915	Europe	Yes	Constituent legislature
2.	Thailand	East	1997	East Asia	Yes	Constituent legislature
3.	Iceland	Western	1944	Europe	Yes	Constituent legislature

4.	Hungary	Eastern	2011	Europe	Yes	Constituent legislature
5.	Kenya	Sub-Saharan	2010	Africa	Yes	Constituent legislature
6.	Colombia	Andean	1991	Latin America	No	Constituent convention
7.	Ecuador	Andean	2008	Latin America	No	Constituent convention
8.	Nepal	Asia South	2015	Asia	Yes	Constituent legislature
9.	Bolivia	Andean	2009	Latin America	Yes	Constituent convention
10.	Dominican Republic	South	2010	South Caribbean	Yes	Constituent legislature
11.	Ukraine	Eastern	1996	Europe	Yes	Constituent legislature
12.	Poland	Eastern	1999	Europe	Yes	Constituent legislature

3.7. Positive Side of Constitutionalism:

Constitutionalism is a system of laws or standards that establish, organize, and specify the limits of a government's power. Therefore, constitutionalism serves as a check on the state's arbitrary use of force and misuse of authority. States are naturally authoritarian, according to Rajiv Bhargava, and the Constitution serves as a check on this authoritarianism. Totalitarianism and authoritarianism are prevented by constitutionalism[12]. Democracy is essential to politicians, and constitutionalism assures that the government does not infringe upon the rights and freedoms of the populace. The legal system, which is currently observed in democracies throughout the world, is guaranteed by constitutionalism. Accepted as an essential component. As the most significant governmental power, constitutionalism supports effective governance & democracy in the state. Allows for the checks and balances on use. It makes sure that no country becomes an elite state. This is especially important in underdeveloped nations because government officials frequently misuse their positions of authority. Most significantly, it makes sure that every person has human dignity and that the state is founded on the rule of law. The privilege has been protected.

*3.8. Democracy and Participation***:**

Voting to act as a public representative or running for office is two of the simplest ways to participate in governance. Voting is the only way to participate in a democracy; There are many other ways to interact with the political system. The proper operation of democracy depends on the widespread adoption of these alternative methods by the general public. The people can't control the government if they only vote once every five or six years, don't vote, and do nothing during the interval. Calling such a regime a democracy is challenging. More information on how to participate can be found on the Citizenship and Participation website. Consider these considerations: what is happening, what decisions have been taken, in the

interest of the people, and especially whether decisions should be formally communicated as Members of Parliament act democratically on their behalf. There are minimum requirements. Your Congressmen are also taking action. They can express their views to organizations working on specific topics or to Members of Parliament or the media. Without public input, leaders are unable to govern appropriately. Trying to hear when alternatives go against individual rights, democratic principles, or even when people strongly disagree with their policies is the best way to achieve it, in my opinion.

3.9. Comparison of Political and Legal Constitutionalism:

A vest, rights-based, but an equitable system that can be tried in courts of law is believed to provide stable and responsible governance and obligate legislators and other officials to follow set norms and procedures. Is. Above all, it stops them from compromising their freedoms in favor of societal bias, administrative efficiency, or short-term benefit. Some scholars contend that a constitution alone can prevent a totalitarian government given that, arguably, no effective constitutional government has simultaneously been a functional democracy. Instead, it attempts to stop democratically elected governments from failing to live up to their principles of treating everyone equally with regard and respect. Therefore, a legal constitution is viewed as a corrective to the basis of a strong political constitution. It is still debatable whether it serves its purpose more authentically or more successfully.

4. CONCLUSION

In all thriving democracies, constitutionalism is a notion that exists, however, officials have figured out how to employ the machinery of government for their benefit rather than for the benefit of the people over time. The government has undermined the formulation of policies whose main goal is the benefit of the general public by allowing backdoor access to corporate interests. The law which was passed to protect the rights of the people is now being used to suppress and deny them. The point is that the Constitution has to be interpreted by those in power as it is unable to explain itself. Institutions that act as shields of constitutionalism are either disintegrating or are inefficient and ineffective. The role of checks and balances has been reduced to the point where it is just academic. The prohibition and influence of money power in the corridors of politics and administration have worsened an already unstable system. The government's apathy and blatant disregard for constitutionalism are fueling a deadly sense of despair, and this downward spiral must be stopped. If prompt action is not taken to check political corruption, democracy will crumble. The gruesome reality of political and bureaucratic corruption in Indian administration demands that this cancer be immediately eradicated from the body of Indian democracy. Residents' demands are growing rapidly, and if they are satisfied, growing frustrations are highly detrimental to the ability of a democratic program to function. In the future, our constitutional principles are facing serious threats from technological change. The fundamental constitutional concepts of freedom of expression, privacy, liberty, and protection against self-blame are being influenced by technological advances.

REFERENCES

[1] M. P. Rovira, “Digital Political Participation and the Digital Divide: Insights from the Cambodia Case,” *Malaysian J. Int. Relations*, vol. 8, no. 1, pp. 66–86, Dec. 2020, doi: 10.22452/mjir.vol8no1.5.

[2] D. Avant and L. Sigelman, “Private Security and Democracy: Lessons from the US in Iraq,” *Secur. Stud.*, vol. 19, no. 2, pp. 230–265, May 2010, doi: 10.1080/09636412.2010.480906.

[3] D. W. Arguelhes, "Transformative Constitutionalism in Latin America: The Emergence of a New Ius Commune," *Int. J. Const. Law*, vol. 17, no. 1, pp. 368–374, May 2019, doi: 10.1093/icon/moz011.

[4] R. Hirschl, "The Nordic counternarrative: Democracy, human development, and judicial review," *Int. J. Const. Law*, vol. 9, no. 2, pp. 449–469, Apr. 2011, doi: 10.1093/icon/mor034.

[5] S. S. F. Regilme, "Constitutional democracy in crisis?," *Democratization*, vol. 27, no. 7, pp. 1324–1325, Oct. 2020, doi: 10.1080/13510347.2019.1687446.

[6] P. Delius, "Chiefly Succession and Democracy in South Africa: Why History Matters," *J. South. Afr. Stud.*, vol. 47, no. 2, pp. 209–227, Mar. 2021, doi: 10.1080/03057070.2021.1855042.

[7] V. Frick, "The Justicization of Politics: Constitutionalism and Democracy in Germany after 1949," *Redescriptions Polit. Thought, Concept. Hist. Fem. Theory*, vol. 22, no. 1, pp. 18–34, 2019, doi: 10.33134/rds.312.

[8] I. Ahmed, "Review Essay: Designing Democracy: Judges, Judicial Review and Constitutionalism in Pakistan," *South Asia J. South Asian Stud.*, vol. 43, no. 2, pp. 369–374, Mar. 2020, doi: 10.1080/00856401.2020.1723042.

[9] O. Sihvo, "The Right to Democracy in the Age of Global Constitutionalism," in *The Finnish Yearbook of International Law, Vol 26, 2016*, Hart Publishing, 2021. doi: 10.5040/9781509954407.0013.

[10] J. L. Černič, "Militant Constitutionalism□: Safeguarding constitutional democracy in the case-law of the European Court of Human Rights," vol. 15, p. 25, 2020.

[11] G. L. Negretto, "Democratic constitution-making bodies: The perils of a partisan convention," *Int. J. Const. Law*, vol. 16, no. 1, pp. 254–279, May 2018, doi: 10.1093/icon/moy003.

[12] Ipleaders, "Positives of constitutionalism in India," 2020.

CHAPTER 14

A COMPREHENSIVE STUDY ON CYBER SECURITY IN INDIA AND NEED FOR STRINGENT CYBER LAWS

Ms. Poojyashree Kumawat, Assistant Professor,
Seedling School of Law & Governance, Jaipur National University, Jaipur, India,
Email Id-poojyashree.kumawat@jnujaipur.ac.in

ABSTRACT:

The term cyberspace refers to the computer-generated Internet, and the rules governing or enforcing this space are known as information technology (IT) law or cyber law. Since these regulations have a global reach, they apply to all users of this cyberspace. In the Internet world, problems like cyberbullying, online fraud, cyberstalking, and child pornography arise with people. The author focuses on the need for cyber law in cyber security for people which provides legal recognition to electronic documents and provides a framework to support E-filing and E-commerce transactions and also provides a legal framework to reduce and prevent cybercrimes. In this paper, the author discusses why people in India need cyber laws, cyber security policies, and types of cybercrimes. It concluded that to keep up with the increasing reliance of people on technology, cyber regulations need to be regularly updated and improved. The worldwide impact of cybercrime has the potential to be quite devastating. As a result, regulations should be updated from time to time and new laws should be made to address contemporary crimes, taking into account the effects of a looser system.

KEYWORDS:

Cyber Law, Cybersecurity, Criminal, Internet, Information Technology.

1. INTRODUCTION

Our online world is a computer-generated worldwide network, and the laws governing it are known as cyber laws; since this is a type of international jurisdiction, all clients of this domain are protected by those laws [1],[2]. Another definition of cyber regulations is the regulatory division that handles issues relating to inter-network data technology in prisons [3],[4]. In short, there is a law that governs how computers and the Internet work [5],[6]. The explosion of Internet commerce has created the need for a vibrant and effective regulatory framework that can also strengthen the penal system, which is critical to the success of electronic commerce [7],[8]. Cyber regulation covers all these government structures and detention facilities. Cyber regulation is important because it touches practically every aspect of online commerce, gaming, and our online environment. In our Internet environment, every action and reaction has a prison or cyber-prison component. As the world becomes more digital and cloud-based, the computer and technology industries continue to grow and change [9],[10]. As technology becomes increasingly involved in business and consumer activities, information leaks, security breaches, hacking and targeted attacks by other cybercriminals continue to occur [11],[12]. The adage that a good offensive is the best defense holds in

computer-related fields. Users, networks, as well as the cloud need to be protected now more than ever as fraudsters become more intelligent.

Any criminal behavior that involves the use of a computer as a tool, victim, or both, is considered a cybercrime. The world of the Internet created by computers is known as cyberspace, and now the rules that apply to this cyberspace are also called IT law or cyber law [13],[14]. Since these regulations have a global reach, they apply to all users of cyberspace. The term cyberspace refers to the computer-generated Internet, while cyber law refers to the laws that apply or are governed by this space. Since these regulations have a global reach, they apply to all people in this cyberspace. It is also possible to think of it as a branch of law that deals with issues relating to the use of information technology mutually. Cyberlaw, simply put, is the body of law that governs the Internet and computers. There is no specific legal framework for cyber law in India; rather, it is a synthesis of intellectual property laws, enforcement of contracts, data protection laws, and privacy regulations, with intellectual property becoming the most important element of information technology laws. Cyber laws are becoming more important as the Internet and computers take over the world and every aspect of our lives. Cyber laws will regulate financial transactions, e-commerce, technology, and information technology in the digital world. All of these judicial systems and administrative procedures are within the scope of cyber law, and they are critical to the success of an electronic business.

1.1. Need for cyber laws in India:

Many crimes and problems arise in today's growing world of the internet and technological methods. To reduce or eliminate these issues, strict regulations must be implemented to protect users' rights, personal property, and copyright and data protection. The legal system of each nation is influenced by its own political, social, cultural, and economic conditions. The need for cyber law has given rise to complex legal issues. Multiple ways of managing and operating electrical equipment. It is quite simple to make copies via the Internet and broadcast them instantly on multiple channels anywhere in the world. Cyberspace is a place where anyone can contribute. For example, a 40-year-old woman may communicate with a 20-year-old abroad often by voice, video, or other means. In a matter of seconds, pirated movies, software source codes, and gaming crack codes can be uploaded to any location around the world. Spreading objectionable content, threatening others through email, breaking into computers and websites, and other ways to damage an individual's reputation and incite enmity between individuals. Today, many people use credit cards for both purchases and payments. Electronic filing is required for all legal documents, government paperwork, business documents, passport applications, and income tax returns.

The present paper is a study of the computer-generated environment of the Internet, often referred to as cyberspace. Additionally, the rules that apply to this area are known as IT law or cyber law. All users of this cyberspace are bound to abide by these rules as they have universal access. It is an area of law that addresses legal challenges arising from the use of inter-network information technology. This paper is divided into several sections where the first is an introduction and the second section is a literature review and suggestions from previous studies. The next section is the discussion and the last section is the conclusion of this paper which is declared and gives the result as well as the future of the study.

2. LITERATURE REVIEW

Simran Mehta [15] et al. have explained that cyber security is the protection you need for any online fraud and theft as well as all your online data. The authors claim that the observational data framework focuses on two aspects: recognizing gaps in legacy innovations and emerging

risks in cutting-edge breakthroughs in media transmission and data. It showed the characteristics of each emerging advancement and the many mediums that malware spread among these new developments. For example, because most of these emerging innovations provide online services, many common attacks abuse program security by using malware hidden inside errors or upgrades to scripting languages to access sensitive information. Lastly, due to the existence of cyber law, there have been many scams, and those responsible have been swiftly identified.

Saurabh Kumar [16] et al. have explained that as the digital world evolves, organizations need a higher level of cyber security. Using the human-organization-technology (HOT) paradigm, the main objective is to identify and address the causes of increased levels of cyber security at the operational level, both from a technical and human resource perspective. The data are analyzed using a structural equation modeling approach based on partial least squares. This indicates that the most important foregoing for increased organizational cyber-security levels are the legal implications and technical measures taken to secure cyber-security. It concluded that it gives managers the information they need to improve the degree of cyber security in their enterprises.

Ranjita Madiwale and Dr.Sona Kumar have explained that after the digital revolution when more people had access to the internet, there was an increase in the number of online crimes committed against Indian women. The major objective is to identify the most efficient preventive precautionary measures to deal with this activity. The author employs good, beneficial uses of technology like cyber security to get rid of the bad that is India's online violence against women. This shows that technology is important in the current environment of increasing crimes against women. Online hunters and grooms use digital platforms to their advantage and apply new tactics to accomplish their malicious purposes. Lastly, due to the increasing scope of online crimes, it is necessary to develop appropriate supervisory legislative measures and efficient law enforcement mechanisms to address the issues.

Sushil Kumar Singh and Neha Rastogi [17] have explained that the number of internet users is increasing rapidly with time due to connectivity between smart gadgets. Service providers are not ready to handle this rapid increase in internet users. The authors have focused on the different categories of cybercrimes and their classification. For example, he discusses the Indian cyber laws that are currently in effect to address cybercrime, the existence of cyber-attack investigation rooms in India and how they work, and how to prevent cybercrime with some solutions. Let's discuss the strategies that are currently in the market. It shows that one of the most prevalent problems in the modern world is cybercrime. On the one hand, people use the Internet for its many benefits, but they also have to deal with the most serious threat cybercrime. Finally, the rapid development of technology has led to a steady rise in cybercrime.

The above study shows that as the digital world evolves, organizations need a higher level of cyber security. The digital revolution, when more people had access to the internet, increased the number of online crimes committed against Indian women. In this study, the author discusses the need for cyber law, cyber security policy, and cyber security policy in India.

3. DISCUSSION

Cybercrime can be defined as any illegal conduct involving computers, network devices, or other connected devices. Cybercrimes can sometimes be committed to making money for criminals, while other times they are specifically committed to damaging or disabling laptops or other devices. In addition, third parties may spread viruses, illegal information, photos, or any other type of content through computers or networks.

3.1. Cyber Laws in India:

Like every other country, India is also concerned about cyber security, having strict cyber laws is even more important as India is one of the largest internet users. There are four main cyber security laws in India, and they have helped broaden the use and access of digital media as well as advanced electronic commerce for the government.

3.1.1. Information Technology Act, 2000:

Most of India's cyber laws are governed under the Information Technology Act of 2000. This law makes it easier to register real-time data with the administration [12] while attempting to legalize e-commerce. The rise in cybercrime has resulted in several amendments. The stringent fines and penalties set up to protect the e-commerce, e-banking, and e-governance industries have been highlighted in the IT Act of Parliament. All contemporary communication tools are now included in the reach of IT legislation. IT Act mandates that cybercrime is subject to strict regulation under Indian law.

3.1.2. Indian Penal Code (IPC), 1980:

As already stated, traditional criminal acts including theft, fraud, forgery, defamation, and mischief will also be part of cybercrime. All these offenses are prohibited under the Indian Penal Code. Consequently, theft and related cyber scams have been defined under the Indian Criminal Procedure concerning the Information Technology Act 2000. Relevant sections include 464, 468, 465, 471, and 469.

3.1.3. Companies Act, 2013:

Stakeholders of the business sector see the Act as an essential legal obligation to carry out and oversee day-to-day operations. The Serious Fraud Investigation Office (SFIO) was created under the Companies Act, which also gave it the power to prosecute Indian corporations and their directors. SFIO became stricter and more proactive in this area due to the company's 2014 Inspection, Investment, and Investigation Guidelines. The law has ensured that all compliance issues such as e-discovery, cyber forensics, and cyber security vigilance are adequately covered under its purview. Strong standards on the duties of officers and directors of the company in affirmation of cyber security are stipulated in the Corporation (Management and Administration) Rules 2014.

3.1.4. National Institute Of Standards And Technology (NIST) Compliance:

By providing a standardized approach to cyber security, the NIST-approved National Conference on Financial Services (NCFS) has established itself as the most trusted organization certified worldwide. All principles, standards, and procedures required to responsibly manage cyber-related risks are incorporated into the NIST Cyber Security Framework. Adaptability and economy are given top priority in this framework. Improving the management, interpretation, and prevention of cybersecurity threats and reducing data abuse, data loss, and resultant restoration costs, contribute to resilience as well as the protection of critical infrastructure [13]. Focusing on planning and achieving important tasks and activities. By demonstrating the legitimacy of businesses making big money. It is beneficial to prioritize spending to optimize cyber security, focusing on legal and statutory requirements. ROI promotes a complete information security program.

3.2. Cyber Security Policy:

All types of users and manufacturers can benefit from the growing goal of an Information and Communications Technology (ICT) cyber security policy. It is one of its components: it

serves as a governance framework, defining and directing activities related to cyberspace security for individuals, small, medium, and large businesses, governments, and non-governmental organizations [14]. This makes it possible for all enterprises to create tailored cybersecurity processes to meet their needs. The policy establishes a framework for protecting networks, information systems, and data in Figure 1. The following is the rationale for policy making:

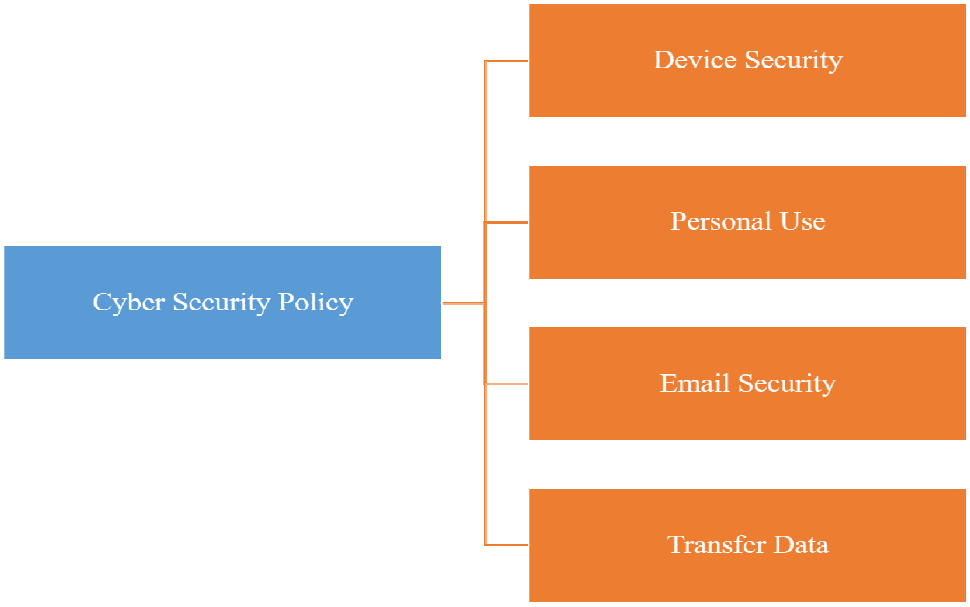

Figure 1: Illustrates the Several Cyber Security Policies in which the Policy Demonstrates Establish a Framework to Protect Networks, Information Systems, and Data.

3.2.1. Device Security:

All equipment and data supplied by the firm must be protected by employees: Password protected (minimum 8 characters) all equipment issued by the company. These include computers, laptops, and mobile devices. Make sure all necessary equipment is turned off before leaving your place of employment. Get approval from an office administrator or inventory manager before removing equipment from the corporate property. Personal passwords should not be discussed with coworkers, friends, senior management, or stockholders. Update your device's security software regularly.

3.2.2. Personal Use:

The study noted that employees may need to use their own devices to access business networks. In some situations, employees are expected to provide management with this material for record-keeping purposes [15]. Company systems must be protected by all employees: All mobile computers used to connect work-related systems are password protected (minimum 8 characters). Invest in antiviral software with tons of features. Make sure your antivirus program is constantly updated. Make sure your gadgets are locked if you plan to leave them alone. Always safely keep all gadgets. Use a private, secure network at all times.

3.2.3. Email Security:

Email security is a significant concern as it can be used to distribute dangerous software such as viruses and bugs, financial fraud, and data theft. As a result, any employee working for a

company should: Verify the validity of each email by looking at the sender's identity and email address. Avoid clicking on links or opening attachments in suspicious emails. Make sure there are no grammatical errors. Avoid using titles as well as links that entice readers to click. Notify IT, staff, if you receive a suspicious email.

3.2.4. Transfer Data:

Company Name is aware of the risks associated with sharing personal information internally or internationally. We anticipate that every employee: should refrain from disclosing personal information to coworkers or others to reduce the potential for data theft. Only use business name networks to send personal information. Get the required power from the top management. Confirm that they have obtained the information and are in compliance with non-disclosure agreements and company name data protection regulations by examining their security protocols. Report any breach, malicious software, or fraud to the IT department as soon as possible.

3.3. Need for Cyber Security Policy:

The Cyber Security Policy establishes rules of conduct for actions such as email attachment encryption and limits on social media use. Given the potential for costly cyber-attacks and security breaches, cybersecurity strategies are essential.

3.3.1. It Increases Efficiency:

The advantage of having a plan is that it promotes sustainability and enables efficient use of time, money, and resources. As per the policy, employees should be aware of their unique responsibilities and what they can and should not do with the personal data maintained by the organization.

3.3.2. It Upholds Discipline and Accountability:

The organization's security policy will encourage any administrative as well as legal action whenever a human error results in a system security breach. Organizational policies act as a contract that proves that a business has taken precautions to protect its intellectual property and both its customers and clients.

3.3.3. A Commercial Agreement can be made or Broken by it:

Enterprises are not required to provide other suppliers with a copy of any policy on information security during a commercial transaction that involves the exchange of sensitive information.

3.3.4. It Aids in Security Literacy Training for Staff:

A well-written security protocol can also be viewed as a guide that tells readers how important it is for them to protect the sensitive information a firm has. It covers a range of topics from choosing the right password to outlining file transfer and digital storage guidelines, all of which improve employee awareness of security and ways to improve it. We use security policies to maintain the security of our network. Most security rules are created automatically upon installation. Additionally, they can customize insurance to suit our specific needs. It reveals the government's methodology and plans to protect the country's cyberspace. It also provides some principles for cooperation between both the public and commercial sectors to preserve data and information systems. Consequently, the policy aims to provide a framework for cybersecurity that will lead to specific initiatives and software developers to enhance cybersecurity security.

3.4. Types of Cyber Crime:

Cyber fraud is a type of cybercrime that uses the Internet to deceive the victim to obtain money or property. Figure 2 shows a variety of different crimes that are committed online under the umbrella of cyber fraud. In this case, apart from theft, the victim is tricked into giving information about property or cash.

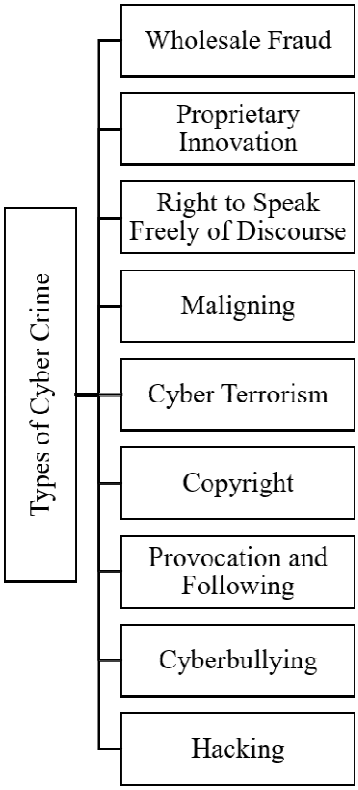

Figure 2: Illustrates the types of cybercrime that include a wide range of specific crimes committed over the Internet.

3.4.1. Child Pornography or Child Sexual Abuse Material (CSAM):

CSAM is broadly defined as any material that contains sexual images in any format and which has the potential to harm children. A clause in section 67(b) of the Information Technology Act specifies that it is illegal to publish or transmit material online that depicts youth engaging in explicit sexual acts.

3.4.2. Cyberbullying:

A cyberbully is a person who uses electronic devices like computers, mobile phones, laptops, etc. to threaten or harass people. Bullying done through digital technology is called cyberbullying. Some examples are the use of social media, chat services, gaming platforms, and mobile phones. This often involves continued action to intimidate, anger, or humiliate the intended victims.

3.4.3. Cyber Stalking:

Cyberstalking is the practice of following or following someone on the Internet or through other technical means. Cyberstalking occurs through text, email, social media posts, and other channels and is often, intentional and systematic.

3.4.4. Online Job Fraud:

An online job fraud scam deceives people who are looking for work that offers them a better position with a higher salary while instilling false optimism in them.

3.4.5. Online Sex-torsion:

Online sexual harassment occurs when a cybercriminal pressures the victim to post private and sensitive information online. Threats are used by these criminals to coerce victims into providing money, sex, or pornographic pictures.

3.4.6. Phishing:

Phishing fraud occurs when an email claims to be from a trusted source but contains a malicious attachment intended to steal a user's data, including their identification (ID), Internet Personal Identification Number (IPIN), card information, expiration date, Card Verification Value (CVV) and other details are included before it is sold details about the dark web.

3.4.7. Wishing:

Viking steals the victim's personal information through his phone, cybercriminals can use social engineering methods to obtain personal information from victims and gain access to their accounts. Vishing assures victims that they are kind by returning the call, as much as fraud and sabotage. Callers often masquerade as representatives of the government, tax authorities, police, or the victim's banks.

3.4.8. Smishing:

Smishing is a type of fraud that, as the name implies, uses a smartphone to trick its victims into dialing a phone number, visiting a fake website, or downloading dangerous software already on the victim's device. Is. Uses text messages sent from.

3.4.9. Credit Card Fraud:

Unauthorized purchases or withdrawals from another person's card are made in the theft of a credit card (or debit card) to gain access to their cash. Credit/debit card fraud occurs when illegal transactions or money withdrawals are made from the customer's account. Fraudulent conduct occurs when a criminal has access to a cardholder's bank card number or personal identification number (PIN). Hackers or unscrupulous employees can take your details.

3.5. Importance of Cyber Crime Laws:

The importance of cyber laws can be illustrated by the following examples: Punishing people who use the internet to engage in illegal activity is a major objective of any cyber law. Where cyber laws apply, significant efforts must be made to successfully pursue crimes including cyber abuse, attacks on other sites or people, record theft, disruption of each company's online operations, and other illegal actions. Action is taken against the person based on the location of the person and how he was involved in the violation of cyber law. Since most cyber-attacks are outside the purview of the law and are not crimes, it is important to prosecute or extradite hackers. Security issues are also related to Internet connections, and some bad guys want to gain illegal access to a computer system so that they can use it to commit fraud in the future. As a result, all rules and cyber laws have been put in place to protect online companies and consumers from unauthorized intrusions and dangerous cyber-attacks. Action against people who commit crimes or violate cyber laws can be taken by individuals or organizations in several ways.

3.6. Cyber Crime and Security:

A set of technologies, processes, and procedures that work together to protect against attacks, damage, and illegal access to networks, devices, programs, and data, is collectively referred to as cyber security. Information technology protection is an alternative name for computer security. Computers and other technology are used by many different types of organizations, such as government, military, businesses, financial institutions, and healthcare facilities, to process, store, and process data on a very large scale. Many of those documents contain sensitive information that could be harmed by illegal access or disclosure, including property rights, financial information, personal information, etc. Protecting the systems that companies use to handle and store sensitive data that is sent across networks as well as others. , Tools are a major topic of cyber security. Therefore, the field of cyber security is responsible for protecting both the systems that transport and store this sensitive data. Companies and organizations, especially those seeking to protect sensitive data (including attacks involving national security, health information, or financial data), are taking necessary precautions in light of the prevalence of cyber-attacks and improvements in such attacks. Proprietary protection of customer and employee data.

4. CONCLUSION

With the increasing dependence of people on technology in India and around the world, cyber laws need to be updated and reformed regularly. Due to the pandemic, there are now too many remote workers, increasing the need for application security. Members of the Legislative Assembly (MLAs) should be extra careful to stay one point ahead of the accused so that they can agitate against them when problems arise. This can be avoided if legislators, Internet service providers, banks, online retailers, and other intermediaries cooperate. Internet and technology have become part of daily life, people spend a lot of time online, which has many advantages but also some disadvantages. Cybercrime is on the rise because of how easy it is for anyone to connect to the internet from anywhere in the world. As technology, as well as Internet access, grows in popularity, so doe's society's reliance company, leading to an increase in the incidence of electronic law-breaking crimes. Although it is impossible to imagine a society without crime, the government must come together to pass laws that can reduce these crimes. It suggested that financial institutions bear the greatest rates of cybercrime, which threatens the economic development of all developing industrial countries and the country. There will never be a direct encounter between both the victim and the perpetrator, which makes cybercrime different. Suspects in cybercrime sometimes operate from countries with weak or non-existent cyber laws, which limit the chances of identification and conviction. Many people have the misconception that cybercrime refers only to crimes committed online or in cyberspace.

REFERENCES

[1] Z. M. King, D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman, and C. Sample, "Characterizing and measuring maliciousness for cybersecurity risk assessment," *Frontiers in Psychology*. 2018. doi: 10.3389/fpsyg.2018.00039.

[2] A. Takano, "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications," *Laws*, 2018, doi: 10.3390/laws7040036.

[3] M. Dawson and P. M. Taveras Nuñez, "Issues in Cybersecurity: Security Challenges and Problems in the Dominican Republic," *L. Forces Acad. Rev.*, 2018, doi: 10.2478/raft-2018-0020.

[4] C. Sabbah, "Pressing pause: A new approach for international cybersecurity norm development," in *2018 10th International Conference on Cyber Conflict (CyCon)*, IEEE, May 2018, pp. 263–282. doi: 10.23919/CYCON.2018.8405021.

[5] S. Mansfield-Devine, "Nation-state attacks: the start of a new Cold War?," *Netw. Secur.*, 2018, doi: 10.1016/S1353-4858(18)30114-4.

[6] J. Kosseff, "Developing collaborative and cohesive cybersecurity legal principles," in *International Conference on Cyber Conflict, CYCON*, 2018. doi: 10.23919/CYCON.2018.8405022.

[7] S. Park, I. H. Kim, J. Kim, and K. L. Lee, "The diagnosis and prescription for cybersecurity in korea: Focusing on policy and system," *KSII Trans. Internet Inf. Syst.*, 2018, doi: 10.3837/tiis.2018.02.018.

[8] T. Pleta, S. Karasov, and T. Jakštas, "The means to secure critical energy infrastructure in the context of hybrid warfare: The case of Ukraine," *J. Secur. Sustain. Issues*, 2018, doi: 10.9770/jssi.2018.7.3(16).

[9] P. J. Morrow, "The New Age Of Cybersecurity Privacy, Criminal Procedure And Cyber Corporate Ethics," *J. Cybersecurity Res.*, 2018, doi: 10.19030/jcr.v3i1.10241.

[10] T. Szádeczky, "Cybersecurity Authorities and Related Policies in the EU and Hungary," *Cent. East. Eur. eDem eGov Days*, 2018, doi: 10.24989/ocg.v331.24.

[11] U. Ķinis, "From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach," *Comput. Law Secur. Rev.*, 2018, doi: 10.1016/j.clsr.2017.11.003.

[12] L. Y. C. Chang, L. Y. Zhong, and P. N. Grabosky, "Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime," *Regul. Gov.*, 2018, doi: 10.1111/rego.12125.

[13] C. Abraham, D. Chatterjee, and R. R. Sims, "Muddling through cybersecurity: Insights from the U.S. healthcare industry," *Bus. Horiz.*, 2019, doi: 10.1016/j.bushor.2019.03.010.

[14] S. Cassotta and M. Pettersson, "Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example," *Beijing Law Rev.*, 2019, doi: 10.4236/blr.2019.103035.

[15] S. Mehta, A. Sharma, P. Chawla, and K. Soni, "The urgency of cyber security in secure networks," *Proc. - 5th Int. Conf. Intell. Comput. Control Syst. ICICCS 2021*, no. Iciccs, pp. 315–322, 2021, doi: 10.1109/ICICCS51141.2021.9432092.

[16] S. Kumar, B. Biswas, M. S. Bhatia, and M. Dora, "Antecedents for enhanced level of cyber-security in organisations," *J. Enterp. Inf. Manag.*, vol. 34, no. 6, pp. 1597–1629, 2021, doi: 10.1108/JEIM-06-2020-0240.

[17] S. K. Singh and N. Rastogi, "Role of Cyber Cell to Handle Cyber Crime within the Public and Private Sector: An Indian Case Study," *Proc. - 2018 3rd Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2018*, pp. 1–6, 2018, doi: 10.1109/IoT-SIU.2018.8519884.

CHAPTER 15

INTERNET AND ITS OPPORTUNITIES FOR CYBERCRIME

Mr. Paras Aneja, Assistant Professor,
Seedling School of Law & Governance, Jaipur National University, Jaipur, India,
Email Id-paras.aneja@jnujaipur.ac.in

ABSTRACT:

Due to its global reach, speed, characteristic trans-linearity, computerization, and ability to automate data handling, the Internet deserves special consideration in criminal research as well as criminal law and strategy. Due to these characteristics, the Internet presents remarkable opportunities for the commission of cybercrimes, which are crimes where PC networks serve as the target or a key tool. This section provides a concise overview of work that has investigated how and why the Internet offers special opportunities to commit crimes, as well as what this implies for the management of (cyber) crime. It presents many typologies of cybercrime and lists twelve Internet gambling components that, when combined, provide an amazing opening for wrongdoing. The section next looks at what is known about cybercriminals, coordinated cybercrime, and digital casualties before briefly looking at the challenges and constraints of enforcing various countermeasures. Although there is little observational research on cybercrime, the speculative experiences and arguments made in the text support the conclusion that wrongdoing is evolving on the Internet. It presents many typologies of cybercrime and lists twelve Internet gambling components that, when combined, provide an amazing opening for wrongdoing. The section next looks at what is known about cybercriminals, coordinated cybercrime, and digital casualties before briefly looking at the challenges and constraints of enforcing various countermeasures. Although there is little observational research on cybercrime, the speculative experiences and arguments made in the text support the conclusion that wrongdoing is evolving on the Internet.

KEYWORDS:

Criminal, Cyber-Crime, criminal activity, Cybercriminals, Cyber Pornography.

INTRODUCTION

The current era of cybercrime is no longer dominated by hackers accessing computer systems just for fun or notoriety. The development and growth of the digital economy have changed the criminal landscape dramatically. High rewards combined with low risks have made digital networks an attractive environment for various types of criminal groups. In the non-digital era, organized crime sought after the safe havens offered by countries with weak governments and unstable political regimes. Today's organized criminal groups can benefit from national jurisdictions that do not have proper legal frameworks and technical capabilities to fight cybercrime. The easiness of communication, anonymity, and the accessibility of tools for illegal operations have transformed cybercrime into a global, fast-expanding, and profit-driven industry with organized criminal groups thriving behind it.

Organized Crime in cyberspace: Changing Structure

Organized criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. While some traditional criminal organizations are seeking the cooperation of e-criminals with the necessary technical skills, newer types of criminal networks operating only in the area of e-crime have already emerged.

The structure of these criminal organizations is different from traditional organized crime organizations. Criminal activities are usually conducted within multi-skilled, multifaceted virtual criminal networks centered on online meetings. These networks are structured on a "stand-alone" basis, as members rarely meet each other in person and sometimes do not even have virtual contact with other colleagues. This sophisticated structure, together with access to the core operations granted only to trusted associates, prevents organized cybercrime groups from being detected and infiltrated by law enforcement.

The networks themselves could involve from ten to several thousand members and could include affiliated networks in their structure. Regardless of the number of members and affiliates, virtual criminal networks are usually run by a small number of experienced online criminals who do not commit crimes themselves, but act rather as entrepreneurs. The leading members of the networks divide the different segments of responsibility (spamming, controlling compromised machines, trading data) among themselves. Some "elite" criminal groups act as closed organizations and do not participate in online forums because they have enough resources to create and maintain the value chains for the whole cycle of cyber-offenses, and therefore have no need to outsource or to be engaged as outsiders into other groups.

Tools and Models for criminal activity

Organized crime borrows and copies business models from the legitimate economy sector. Cybercriminals employ models similar to the B2B (business-to-business) for their operations, such as the highly sophisticated C2C (criminal-to-criminal) models, which use very effective crime tools available through digital networks. The computer systems' vulnerabilities and software are exploited to create crimeware such as viruses, Trojans, and key loggers. These crimeware tools offer criminal groups the flexibility of controlling, stealing, and trading data.

The development of botnets, and networks of compromised computers running programs under external control, transformed some types of cybercrimes such as phishing into the worldwide underground ecosystem run by organized crime. The estimated financial gain of these criminal groups ranges from tens of thousands to tens of millions of dollars. The trade of botnets has also become a high-revenue activity that could be also linked to organized crime. The botnets' costs are relatively low compared to the criminals' financial gain and to the damage to individual consumers and businesses, as well as to the financial health, reputation, and trust in online transactions as a whole.

Crimeware is also used to deploy Crime-as-a-Service business models that represent the system of trading and delivering crimeware tools. Data-supplying models are also used to share the tools to commit cybercrimes. For instance, by creating "customer" systems where instruments are available on demand, "users" just log into the server and choose from the range of tools suitable for fraud, phishing, and data stealing and then download them. When user data is stolen, criminals can use crime ware servers to commit organized attacks. Crime ware servers allow to control of compromised computers and manage the stolen data.

Prevalence and Perceptions of Cybercrime

The specific predominance of cybercrime is obscure. Convictions for cybercrimes are still generally interesting (contrasted with different violations), albeit that doesn't mean cybercrime isn't common [1].

There should be a high 'dim number' of undetected, unreported, unresearched, or unsettled cybercrimes, because of the intangibility and intricacy of computerized follow and an overall hesitance of business casualties to report inspired by a paranoid fear of notoriety harm. Wrongdoing casualty studies have as of late remembered inquiries for Internet wrongdoing, frequently restricted to misrepresentation and unlawful or hostile substance; they will generally bar malware and other 'center' cybercrimes since these are challenging to perceive for normal PC clients. Numerous measurements are distributed of computer□security episodes, outstanding infections, and other malware and phishing endeavors. Nonetheless, these frequently come from security organizations with an interest in selling, e.g., anti□virus programming, and ought to hence be taken with a (huge) spot of salt. Another confounding variable is the 'folklore' of cybercrime taken care of by well-known pictures in films and books, with a cliché programmer as the prototype cybercriminal [2]. Such famous discernments can be distant from the real world.

By the by, the general pattern in the writing is to assume that (a lot) a bigger number of cybercrimes should happen than is exactly settled, regardless of whether research endeavors neglect to reveal insight into the 'dull number'. Cautions against the problem of our convictions about cybercrime's commonness: 'We are stunned by cybercrime, yet in addition hope to be stunned by it since we anticipate that it should be there, however - confusingly - we seem, by all accounts, to be stunned on the off chance that we are not stunned (if we don't find it!).'

Typologies of cybercrime

To comprehend cybercrime, it is valuable to make a few qualifications since the inspirations and modi operandi of culprits might vary for different sorts of cybercrime. The most widely recognized differentiation is between the Internet as a device and as an objective. The European Commission (2007, accentuation added) characterizes cybercrime as 'criminal demonstrations perpetrated utilizing electronic correspondences organizations and data frameworks or against such organizations and frameworks'. Other than PC networks as instruments or objects of wrongdoing, Donn Parker (1973) currently brought up a third kind where PCs are the climate of wrongdoing, in the feeling of a pretty much-unbiased foundation for wrongdoing. The typology of the Internet as an item, instrument, or climate is reflected in what is presumably the most valuable categorization of cybercrime to utilize today: the rundown of meaningful wrongdoings in the Council of Europe's Cybercrime Convention. The Convention condemns:

1. Offenses against the secrecy, uprightness, and accessibility of PC information and frameworks; incorporate unlawful access (hacking), unlawful block attempts, information obstruction (for example infections), framework impedance (e.g., denial□of□service assaults), and abuse of gadgets (e.g., having programmer programming);
2. Computer□related offenses; incorporate falsification and misrepresentation;
3. Content□related offenses and copyright offenses; the previous covers kid porn (bigotry is remembered for a different Protocol to the Convention).

An alternate, more sequential, typology is presented by Wall [3] zeroing in on the developing open-door construction of cybercrime. The origin of cybercrimes comprises conventional violations where (stand□alone) PCs are just an instrument; these are 'low-end' cybercrimes. The subsequent age, from the 1970s onwards, comprises wrongdoings worked with by neighborhood or worldwide PC organizations; these are still generally conventional violations, however, they bring about new globalized open doors and jurisdictional issues. The third era is 'valid violations completely interceded by innovation', comprising a 'step□change in the change of cybercrime' [4]. These are 'very good quality' and sui generis cybercrimes that wouldn't exist without the Internet. The focal point of this typology isn't such a lot of the job of the Internet as a device or target, however how wrongdoing itself is being changed by the Internet, developing into new structures with various examples of wrongdoer association and offender□victim relations.

In this regard, the inquiry emerges whether a fourth era is arising, where cybercrime happens through or on the Internet, yet in totally virtual spaces, for example, gigantic multi□player web-based role□playing games (e.g., World of Warcraft) and virtual universes (e.g., Second Life). Ought to manhandle perpetrated in these virtual spaces, like taking virtual swords, having intercourse with a young□looking symbol, or mishandling a symbol, be treated as a new, sui generis kind of wrongdoing - a fourth era of 'virtual wrongdoing' or as a better approach for carrying out customary violations (second era), or not as wrongdoing by any means since it is simply 'virtual' and not 'genuine' or because different normal practices apply in virtual networks? Current writing appears to lean towards the last option draws near: on the off chance that there is some type of genuine (i.e., non□virtual) hurt which isn't clear with 'virtual wrongdoing' the way of behaving can be treated as a customary offense. One more important arrangement depends on various inspirations. Thomas and Loader (2000) recognize programmers and phreaks (inspired by interest), data vendors and hired soldiers (spurred by monetary benefit), and fear mongers, radicals, and degenerates (persuaded by political or social action). For a few different orders, see Walden [5].

Risk factors of cybercrime

The opportunity structure for cybercrime may be explained in part by several aspects of the Internet. It is a worldwide network that enables quick contacts, has a decentralized networked structure, and is built on the digital representation of information. These Internet characteristics serve as the foundation for 12 distinct, connected risk factors that encourage cybercrime. On the Internet:

1. Has a worldwide reach, allowing offenders to locate the most susceptible machines and victims anywhere in the globe without leaving home or the Internet café next door [6];
2. Enables decentralized, flexible networks where offenders can (loosely) organize themselves to divide labor or to share skills, knowledge, and tools (cf. infra, section 3.3);
3. related to this, leads to deterritorialization, which implies that cybercrime is almost by definition international, with consequent legal challenges of jurisdiction and cross-border cooperation;
4. facilitates anonymity, at least for offenders who are aware of and make an effort to use anonymization tools like remailers and torrent networks; however, even less tech-savvy offenders are (or feel) relatively anonymous when they operate from behind an IP number, email address, or phony Facebook profile that is frequently difficult to trace to a specific individual [7];

5. makes it possible for offenders to contact victims remotely, eliminating any social obstacles they may encounter in face-to-face interactions; as a result, cybercrime entails "anonymous, networked, and rhizomatic exchanges between perpetrators and victims" (Sandywell, 2010: 44);facilitates manipulability of data and software with minimal cost because it is based on digital representation (allowing for copying without loss of quality, and altering without visible traces) and because the Internet was built as an open infrastructure with intelligence at the endpoints to foster innovation by end□users;
6. 6. enables the automation of criminal processes, allowing a single piece of Internet-launched software to replicate and attack millions of computers at once - but also over longer periods - and allowing so-called "script kids" to easily modify basic software, such as a sample virus, to create a new virus;
7. When a virus has far more serious consequences than a curious script kiddie anticipated, or when a comment or (sex) photograph posted online acquires a global and permanent reach, for example, "harassment writ large in cyberspace - expanded so drastically in target, scope, and reach - has a far greater impact than any physical harassment," it can increase the scale of a crime from a minor annoyance to major harm.
8. enables the accumulation of several little profits, such as when using the salami approach (which involves stealing 0.5 cents from 10,000 bank accounts 1,000 times); This de minimis dilemma may be one of the largest obstacles for cybercrime as it lessens incentives to report, investigate, and punish the crime more generally because cybercrime frequently involves several victims with just minor damage to each one.
9. promotes an information economy where information has become a valuable asset in both the legal market (such as music, movies, software, and books) and the black market, where credit card numbers, personal information, and passwords are traded to facilitate fraud and theft [8]; has structural restrictions on capable guardianship that can act as a social or technological barrier to committing a crime and have quick innovation cycles that allow for new ideas to be developed.

The combination of these characteristics or risk factors, authors generally agree, is what makes cybercrime a unique challenge and suggests that the Internet has an impact on changes in crime. This is true even though they tend to highlight different subsets of these characteristics or risk factors as the major factors to take into account. For instance, Balkin and Kozlovski's summary in 2007 reads: "Digitization, anonymity, interconnectedness, decentralization, and interdependence shape the online world as it is now known. According to Sandywell [9] "When combined, these features create ubiquitous digital platforms that facilitate information-based borderless crime on a global scale and thus prefigure the emergence of a situation of constant information warfare." This means that they structure the opportunities for crime and the ways that people commit crimes and breach network security.

Cybercriminals

Hackers and their hats

It is customary, at least in sociological and technical literature, to distinguish between two basic types of hackers: good guys, called ‘ethical hackers’ or ‘white hat hackers’, and bad guys, called ‘crackers’ or ‘black hat hackers’. For many, the term ‘hacker’ retains the aura from the 1980s and early 1990s when hackers wearing white hats played a crucial role in the development of the Internet by testing systems [10]. This generation shared a code of norms, a ‘hacker ethic’, to enhance information security, freedom of information, and access to technology, and ultimately aiming at improving the Internet and the world at large.

Subcultures within the hacker community, however, differed in the background, some being simply curious whiz kids, some being 'utopians', and others being fiercely anti-establishment 'cyberpunks'. The latter groups did (and do) not mind harming information systems if they thought it contributed to their goal, and hence, tended to be disruptive in a society dependent on information systems[11]. Moreover, with the Internet reaching the mass public in the 1990s, other groups started to use hacking driven by other motivations, such as financial gain, terrorism, and other types of 'hacktivism'. Deviating from the Volume 1 E.J. Koops 742 'hacker ethic', such perpetrators were termed 'crackers' by the self□righteous 'ethical hacker community. But in fact, it has become difficult over time to distinguish between clear shades of white and black in the hats of hackers: 'hacking has developed far beyond the original first generation system hacks to reveal a broad array of activities and motivations. Under scrutiny,this range of behaviors is found to represent a spectrum of qualitatively different types of trespass, from intellectually motivated acts at one end to politically or criminally motivated trespass at the other'.

The dominant discourse of law and policy does not distinguish substantially between the various motivations of hackers: regardless of the color of the hat, hacking unless with explicit consent when a company orders a hacker to test their system is generally considered a criminal act. There is justification for this, since for a victim of illegal computer access it is difficult to determine what the hacker has done and why, and the integrity of the computer system is corrupted [12]. It is also the result of the "established institutions of cyberspace [having] enlisted the power of conceptual schema in their quest for order and control" that nowadays, hacking is "imbued with a normative meaning whose core refers to harmful and menacing acts, and as a result, it is virtually impossible to speak of, let alone identify, the hackers that engage in activities of significant social value".

Types and characteristics of offenders

Even though hackers are now generally seen to wear grey to black-colored hats, there are still distinct differences between subgroups of hackers, and the stereotypical hacker is far from the only cybercriminal on the block. Some characteristics can be given of cybercrime offenders, although it should be stressed from the start that, similar to prevalence data, little empirical knowledge is available of offenders (except for a few special types, such as cyberstalkers and child pornographers) (Van der Hulst & Neve, 2008). Nevertheless, based on the literature study and theory, some tentative insights can be provided.

On average, cybercriminals tend to be male, white, and young, but the variation in offender groups is rising. Cybercriminals are, again generally speaking, also expected to be to some extent technical savvy, have a disregard for the law or a feeling of being above or beyond the law, have an active fantasy life, be a control freak or risk□taking, and have strong if differing motivations. But types of cybercriminals differ, depending on their aims, methods, or skills. Hackers are for example characterized according to their skill as 'gurus', 'wizards', or 'samurai' (whitish hats with great skills) or, conversely, as newbies, 'clubs', or 'script kiddies' (whitish to blackish hats with no or low expertise) (Wall, 2007, pp. 55□56, 65□66). The most extensive and most interesting typology is the 'hacker circumflex', in which Rogers (2006) distributes nine hacker types in a circle consisting of four quadrants of different motives: The Internet First Part: Risk Factors - Environment

1. Revenge against persons, organizations, countries, or continents;
2. Financial gain;
3. Curiosity knowledge, sensation, intellectual challenge;
4. Fame media attention, boasting, and popular hero.

Nevertheless, as noted by Van der Hulst and Neve (2008: 112), this model is still only a hypothesis that has to be experimentally tested. Additionally, other forms of incentives, such as those that are carried out 'for pleasure,' for sexual arousal, or political reasons, could also be at play (Cross, 2008: 94; Wall, 2007: 62–63). Based on a study of the research, Van der Hulst and Neve (2008: 106–107) distinguish between three fundamental offender categories linked to various motivations:

1. Young male criminals, who hack for fun, curiosity, or peer respect;
2. Ideological hackers, who are intelligent and eager to learn, some of whom are obsessive, anti□social, or have a minority complex;
3. Financially□motivated hackers, from various backgrounds

The Doctrine of Mens Rea & Actus Reus in Cyber Crime

After considering all factors the two most important elements of wrongdoing are mens rea and actus rea. The Latin phrase Actus Reus means "Such consequences of human lead as the law attempts to avert." [13]. A wrongdoing must be committed or excluded to be considered. When all is said and done, it denotes "A liable attitude of mind"[14]. The psychological factor influences the second important component of wrongdoing. While the perspective characterizes the demonstration as "reus" and hence an offense, the demonstration proceeds as before. Almost all crimes involve proof of a mental component of some kind[15]. When it comes to cybercrime, determining the men's rea is quite difficult.

One should consider the perspective of the programmer in cybercrimes and if the programmer was aware that the admission was not authorized. As a result, the programmer need not anticipate a "Specific Computer," as long as "any PC" was the target of the unauthorized access, it would suffice. Where the programmer is an outcast and has no else to go, mindfulness about him is easier to display. It becomes challenging to explain how the programmer exceeded his cut-off points and was even aware of how he is beyond them now that he has limited power as a representative of a company. Actus Reus because the entire demonstration is carried out in a mysterious atmosphere, cybercrimes have evolved into a test. The perpetrator may leave a few footprints in the real machine, but it becomes a difficult task for the police to prove it in court since it must be in the actual machine or at least in a place where it can be used as evidence.

Cyber Pornography

The term "porn" is derived from the Greek words "porne" and "graphene," and it refers to literature that elaborates on whores, alludes to any show-stopper, or deals with sex and sexual themes. The phrase "sexual entertainment" is extremely difficult to define, and there is no legal definition for it because every country has its traditions and customs. While it is legal to perform sexual entertainment in some countries, it is against the law and wrong. In simple terms, digital porn is the practice of creating, displaying, communicating, importing, or disseminating lewd or sensual material online. Traditional explicit material has been mostly replaced by online/computerized obscene stuff since the advent of the internet.[16] There is no accurate or valid definition of pornography. Depending on how the general population, standards, and characteristics react to the explicit material, sexual entertainment has different meanings.

All things considered, the reason we lack a real definition is that there are no universally accepted standards of morality or culture on earth, nor are there universal laws defining sexual entertainment. The perception of filth and obscenity fluctuates from one nation to the next. While vulgarity and sexual entertainment have separate meanings, they are related.

Similar content that was illegal in some countries could be legal in others. The word "sexual entertainment" is not defined by Indian law, and so is not governed by it.

Sex sells extremely well in the developed world, and the sexual entertainment market today is larger than any other organization or combination of organizations on the planet. The globalization of the internet has opened up a new market for pornography. The pornography industry finds the best place on the internet to disseminate offensive material. According to the 2010 Web Channel Audit Report, there are 4.2 million websites worldwide that sell pornography. There are 68 million daily web index requests and 72 million monthly visits to adult-only locations. 42.7 percent of all internet users in total view explicit content online [17].

Before the general public had access to the internet, or in earlier years, videotapes and DVDs were the most popular means of disseminating porn. However, as the internet is widely available, it quickly overtakes other media as the most popular way to provide clients with the comfort of their own homes with sexual entertainment. A person can now successfully watch an image or a video on the internet if they avoid indecent stuff due to partner pressure or shame. More prominent access to porn was made possible by the rise of sexual entertainment websites that provided pictures, videos, and web-based media, including live webcam access. Making and distributing explicit materials online has become easier thanks to data innovation. For instance, the material can now be shared instantly throughout the entire world, and the geographical restrictions that once made it difficult for unfamiliar distribution to reach nearby areas have vanished[18].

CONCLUSION

It has always been difficult to combat cybercrime. It crosses international borders and encompasses several jurisdictions. For cybercriminals, committing crimes online is simple, quick, and generally safe: Through computer networks, intangible computer data may be swiftly and readily moved from one area to another, without the criminal having to be there in person. Due to the international scope of the crime, cybercrime investigations require a lot of time and effort. 70 Automated assaults, anonymous communication, and training locations: Members of the network who are targeting victims throughout the world may be in one country while crimeware servers are in another.

The detection, investigation, and prevention of e-crimes committed by organized criminal groups require cross-sector cooperation on the national level as well as international cooperation in addition to strengthening current legal frameworks, modernizing outdated legislation, and harmonizing laws on a global scale. 71 Given that organized cybercrime appears to be a dynamic target, thorough knowledge, and a forward-looking strategy are needed. International cooperation between nations is essential in the borderless web. While some lack the technological know-how or are constrained by the law, some jurisdictions simply lack the resources to counteract the actions of organized cybercriminals. It is crucial to have a shared awareness that no nation can be secure on its own in the global ICT network. Only on a worldwide scale can the issue of harmonization of the law be resolved.

Cybercrime may be evolving into an organized, unlawful sector with syndicates that are extremely sophisticated and difficult to track. As a result, likely, criminal organizations will soon dominate the cybercrime landscape, as already-established international cybercrime networks will multiply opportunities and expand to a global scale by taking advantage of legal frameworks' weaknesses and looking for safe havens in nations with limited resources. This issue should be addressed by creating long-term responses that include coordination and harmonization of efforts on both the national and international levels.

REFERENCES:

[1] "Smith et al., 2004, pp. 25□29".

[2] "(Wall, 2008a; Wall, 2008b; cf. Jewkes and Yar, 2010, pp. 104□166)".

[3] "(2007: 44□48)".

[4] "(Wall, 2007: 47)".

[5] "(2008, pp. 21□23)".

[6] "(Yar, 2005: 421)".

[7] "(Sandywell, 2010, p. 44)".

[8] "(Wall, 2007: 32)".

[9] "(2010: 44–45),".

[10] "(Wall, 2007, p. 55; Sterling, 1994)".

[11] "(Wall, 2007, pp. 55□56)".

[12] "(Furnell, 2010, 176□177)".

[13] 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".

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

[15] T. Fatima, "Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68".

[16] "http://blog.ipleaders.in/cyber-pornography-law-in-india-the-grey-law-decoded/."

[17] "http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html".

[18] D. Gorman, L. and Maclean, "Media and Society in Twentieth Century, Blackwell publishing, 2003.".

CHAPTER 16

A STUDY ON CYBERSECURITY IS ENOUGH AWARENESS

Dr. Jyotsna Yadav, Assistant Professor,
Seedling School of Law & Governance, Jaipur National University, Jaipur, India,
Email Id-jyotsna.yadav@jnujaipur.ac.in

ABSTRACT:

Information security awareness can play an important role in facing cyber-attacks by intruders. The main goal of this paper is to analyze the information security awareness among academic stars, researchers, undergraduate students, and employees within educational environments in the Middle East in an attempt to understand the level of awareness of information security, the associated risks, and the overall impact on the institutions. The results reveal that the participants do not have the requisite knowledge and understanding of the importance of information security principles and their practical application in their day-to-day work. This situation can however be corrected through comprehensive awareness and training programs as well as adopting all the necessary safety measures at all levels of the institution to ensure that the students, academic star, and employees are trustworthy, technology savvy, and keep their data safe. Without such training programs and awareness, there will be negative consequences on IT systems and their application usage, as well as on users' security now and in the future. From the weaknesses identified in this survey, some essential recommendations are put forward to remedy the situation.

KEYWORDS:

Cybersecurity, Data, Media, Password, Systems.

1. INTRODUCTION

Most activities are now completed online with little to no physical interaction, making network security risks a serious problem for many organizations and individuals. As a result, the existence of the web has fundamentally changed how people learn, gather knowledge, and produce information [1]. This new way of doing things has provided an additional method for people to share and participate in cultural activities. Although the creation of the internet was widely acknowledged as one of the most significant technological advances ever achieved and one that is being used on a global scale, it also has drawbacks that result from customers using it improperly. The use of the internet has brought with it several digital risks, such as digital dependency, individual data openness, individual data openness, and online misrepresentation slavery [2]. Because they allow access to their internal operations, many associations are always the target of numerous attacks. An assessment conducted by the Serianu organization found that the banking and telecom industries lost close to $649 million. This analysis also reveals that $3.5 billion was lost across Africa, with Nigeria being one of the most affected nations. This demonstrates that many associations fall short when it comes to network protection awareness programs.

With a population of over 181 million people, 60% of whom are young, Nigeria has 92,699,924 Web users. According to [3], 97% of African organizations spend less than $10,000 on digital protection, with Nigeria being the most notable. Furthermore, 97% of

respondents say they require the ability to recover from digital attacks, and 64% of respondents say their representatives need training in network safety. Unfortunately, Nigeria has the highest overall percentage. This showed that there is a national lack of awareness about cyber security. Higher education students are active web users; many of them rely on it for information and online amusement as well [4]. By exposing children to online dangers and risks for an unexpectedly long period, the web may make students flimsy. This investigation aims to ascertain the knowledge and awareness of network security among Yobe State College's software engineering understudies. The following are the objectives of this essay: - To investigate the online safety knowledge of male and female students at Yobe State College Damaturu, Nigeria's software engineering program.

1.1.Objectivity and Purpose of the Review

The modern world is growing more intelligent, and programmers are improving greatly at retrieving information. Everyone in the world now uses a pocket PC. Cybercrime is therefore growing worldwide because ofthe increased use of online entertainment, dispersed storage, and online installments. Digitalization is something we cannot halt; we must keep up with the times. In any event, being watchful and protecting ourselves means a lot. The more we try to hide our secret phrase, the more inclined programmers are to find it. The individual and monetary information of the shoppers is all over. The PCs and PCs that we are utilizing isn't away from the assault of malware, emancipate product, and phishing. Phishing assaults are chiefly focusing on government-backed retirement numbers, MasterCard data, and ledger information of the clients. It is likewise a need to feature that the training area is positioned rearward as far as network protection execution when contrasted with other significant areas or enterprises. Furthermore, there lies the requirement for understudies to foster a self-obligation to upgrade their security. "Uttar Pradesh has detailed a more than 90% ascent in the contribution of understudies in Digital related violations beginning around 2012" Season of India.

According to NCRB (Public Wrongdoing Report Department), 318 of the 812 students who admitted to participating in cybercrime cases across the nation were from the University of Punjab. Thirty people were connected to cybercrime in 2012; forty were in 2013. Similarly, the figure increased to 62 out of 1223 capture. It was astonishing to learn that the majority of cybercrimes are sexual and are committed by friends or young women/sweethearts using online entertainment to exact revenge. The true number of cases is far more than the number of cases that have been publicly disclosed, which another fact is. Many of the survivors' guardians are reluctant to reveal information against the accused because they don't want to jeopardize their reputations and standing with the public. According to the words of well-known network safety expert Rakshit Tandon, "School-aged children and students are the ones who get arrested the most in cybercrime cases across India. We identify a trend of retaliation, sexual deceit, extortion, and other cybercrimes committed by youngsters since they are the heroes of the digital or web era. The problem is that our educational system has not taught students proper netiquette, digital hygiene, and morals. Recently, they were handed open to high-quality innovation and playable devices. "A total of 2,208 instances of cybercrimes were reported in Uttar Pradesh, of which 186 cases involved online fraud, followed by digital coercion, sexual impersonation in, unsavouriness or embarrassment in 112, incitement to commit crimes against the local community in 115, theft in 59, and extortion in 41. But in the state, there were 1154 occurrences of internet extortion for monetary gain, which was the highest number.

Most of the time, criminals using digital assault use network traffic, phishing emails, and client profiling to launch an attack (Moallem, 2019). Exactly 4.9% of students had used the

internet to follow. According to Al-Janabi and Al-Shourbaji (2016), "the accessibility of technology has offered an application to teaching either on the web or unconnected, college students may obtain too much info indiscriminately, which also helps them with developing their learning." "Preventive actions and data security awareness increase security performance directly related to each other" (Knapp, Marshall, Rainer, and Passage, 2006). "There are connections between data on data security and how people behave that may be strengthened" (Kruger, Drevin, and Steyn, 2010). Cyberattacks can be prevented by increasing awareness of digital security. "Projects for network protection should be designed such that such components are included, with these components' security techniques and rules defined by the association to get the best outcome" (McDaniel, 2013). "College frameworks have continuously been pursued due to free access to data and a significant amount of force worth interacting" (Katz, 2005).

1.2.Background

Africa, one of the areas that face the most noteworthy paces of cybercrime, experiences significant monetary misfortunes because of cybercrime (Bada, Von Solms, and Agrafiotis, 2019). Digital lawbreakers utilize new and imaginative ways of tricking individuals to go after them with unlawfully acquired data about them by making customized assaults (Zeltser, 2019).

1.3.Weakest Link

Organizations frequently use cutting-edge security technologies to protect their data and only train their security professionals, but little thought is given to the attention to data among the data's actual clients. Directed research showed that the majority of PC users lack data security knowledge due to poor awareness. Although the human element is thought to be the most susceptible link in data security, the main goal of data security mindfulness is to enlighten customers about a certain situation or reality to make them aware of data security (Alotaibi and Alfehaid, 2018).

To support an organization's vision and strategy, security training, preparation, and awareness (SETA), as well as network security skills, should be crucial for the association's management outlook.

This includes the cost of security and the requirements for it. The success rate of such events will slow down to protect the association's resources, assuming staff members have the necessary knowledge on how to respond in hazardous situations. Although academic institutions train students for the workforce, they ignore their familiarity with data security because they believe that their future managers will be in charge of these matters. Students may be aware of the fundamentals of data security, but they are not schooled in the security protocols of a business. Educational institutions should give kids the necessary security awareness training so they may grow up with a consistent, secure way of acting.

Furthermore, the lack of CSA might be perceived as putting customers in danger. Despite being the most flexible efforts in an organization, CSA programs are rarely utilized by organizations. In a 2016 review, ütçü, Testik, and Chouseinoglou found that the members' degree of mindfulness was not high and that to safeguard clients from potential threats, it is crucial to encourage client behaviors. While providing network safety measures in schools in affluent nations is expensive, most agricultural nations don't have this problem.

1.4.Social Media

Due to the popularity of the internet, which includes the use of e-mail and social media, the length of online activities rises. A security culture should be built for an institution's members via various delivery mechanisms to secure data. ISA may also be communicated via electronic communications like social media. The CSA should communicate using the same channels that consumers use often, such as social media.

1.5.Initiatives to Improve Cyber Security Awareness

To improve ISA, conventional techniques such as posters and newsletters or internet communications techniques might be employed. Emails may be used to inform individuals of potential cyber security dangers that they may encounter (Dugan, 2018). Information security measures should relate to a person's daily life, such as children's safety on social media, to persuade individuals to use them.

1.6. Advantages of Cyber Security Awareness

To fully protect data resources, customer viewpoints, and behavior need to be combined with information. It implies that clients are aware of the risks they face and can take appropriate action to reduce those risks (Martin, 2014). ISA is a crucial step in creating a secure digital environment where clients may use innovation for activities. Security awareness is just meant to raise awareness of security, not to prepare. The first step in reducing the number of risks is to practice mindfulness. Since clients are less likely to experience threats when they are aware of how they could occur, mindfulness should be promoted. Because end users play a crucial role in ensuring the security of businesses and data systems, awareness of digital security is to ensure that customers are aware of the risks they may face while engaging in online activities. Clients are helpless against digital attacks, but CSA can reduce the number of possible fatalities [5]. Kruger and Kearney (2006) used three criteria, specifically information, attitude, and behavior, to assess the degree of ISA. These three parts can be characterized as

(i) What an individual knows,
(ii) how does the individual feel about the point,
(iii) What an individual does about the subject. Consequently, CSA ought to grow the information on individuals about digital protection and improve an inspirational perspective and conduct towards network safety.

The point of safety and mindfulness is to build a culture of safety where the clients are completely mindful of their activities to safeguard data and administrations [6].

1.7.Lack of Cyber Security Awareness

People often fail to understand security risks since they don't feel in danger (West, 2008). Social factors influence how customers behave with ISA, and older people have a harder time adapting to new technologies.

Understudies' lack of awareness can be attributed to a lack of safety education. Students need to understand security risks, the problems that these risks might cause, as well as the best ways to mitigate these harms if they do occur [7].

1.8.Objective

To identify the level of basic knowledge of cybersecurity among prospective teachers.

1.9.Methodology

A questionnaire about cyber security knowledge was used to collect data from Aligarh Muslim University's prospective instructors for the study, which is a descriptive survey. Purposive sampling was used to gather the sample.

1.10. Sample

Aligarh Muslim University's Department of Education's 100 postgraduate prospective teachers, 60 of whom were women and 40 of whom were men, were chosen for the study using a purposive sample approach.

1.11. Tool

The themes on which survey questions are based include a range of cybersecurity-related subjects, such as social media use, virus assaults, and password strength. Using a Google Forms online survey, the students were provided access to this survey. The survey question covers user names, passwords, dangerous defense, computer viruses, phishing, pop-up windows, and fake social network contacts.

2. Description of the Module Exercises

The three sections of the e-learning curriculum are called Password Security, Social Engineering and You, and Browser Security. Each unit aims to enlighten the user about the subject and pique their interest in it through interactive tasks including password entry, viewing brief news clips of pertinent happenings, and/or visiting fascinating websites. The descriptions for the exercises in the module are provided below.

2.1.Password Security

According to Tozzi, the largest threat to someone's privacy still comes from using weak passwords. People continue to often use weak passwords that are simple to crack, leaving the user vulnerable to data theft and other security issues [8].

Three password exercises are included in this unit:

a. The first part of this activity teaches the user what constitutes a strong password. After that, it prompts the user to input a potential password, examines it, and displays a table with details on the components of a strong. password it contains and those it lacks as well as an estimate of how long it would take to crack the password based on the characters it contains.
b. Password Cracking: This exercise builds on the first by briefly describing how dictionary and brute-force attacks operate. It also asks the user to enter a password (limited to 5 lower-case letters for the sake of speed) and provides an estimate of how long it will take to break the password using each method.
c. Default Passwords: Following a description of how certain devices have a default password for quick setup and accessibility, this exercise shows the user a news clip cautioning them about using the default password on a camera. Additionally, a website listing default passwords for various devices, such as webcams and routers, is linked in the exercise.

2.2.Social Engineering

This chapter focuses on the practice of "phishing," which involves deceiving users into providing their login credentials for secure services. The sheer number of people who fall victim to phishing scams is astonishing. In a survey of 150,000 phishing emails conducted by

Verizon partners, it was discovered that 11% of receivers opened attachments and 23% of recipients clicked on links, according to the Verizon Data Breach Investigations Report (2015).

This unit in our module includes two exercises:

a. *Phishing and You:* This activity begins with a description of phishing and lists the telltale indications of a phishing assault in an email. Then it illustrates a tactic employed by attackers in which a link's visible URL and the URL that the browser goes to when that link is clicked are two distinct websites.
b. *Fake Websites:* This exercise shows an attack strategy where a user is sent to a website that appears to be extremely similar to the website listed in the link but is an entirely different website that is purposefully copying the authentic site. This website may be dangerous if it requests user credentials!

2.3.Browser Security

Many people's windows onto the internet are their internet browsers. People use web browsers to conduct the majority of their online activities, but they don't control them; they frequently accept the default settings and are unaware that they may be changed. This exercise offers succinct definitions of popular browser features including cookies, scripts in code, and plugins that may raise security issues. Additionally, it offers users straightforward instructions on how to access the security settings on popular browsers like Chrome, Firefox, and Internet Explorer. Then, users are made aware of the official help pages for these browsers, which offer detailed explanations of all the choices available for their security settings [9].

2.4.Description of the Survey

A 20-item self-developed survey was used to gauge participants' awareness of and concern for cybersecurity. Users were mostly asked to rate how aware they were of things like creating passwords, using the internet, and clicking links. Users were asked to complete a brief survey as part of the post-test to offer feedback on the module's positive and negative aspects as well as recommendations for improvement (s).

2.5.Contextual Influence of Cybersecurity

In evaluating the setting of network protection, analysts for instance, Nam, 2019; Mueller, 2017) have seen network safety-related ideas as significant parts of understanding how to close the information hole in client consciousness of network safety. This is basic in understanding the exploration issue in my review which was the absence of information and comprehension of the degree of consciousness of network protection and the job and viability of workers preparing to upgrade online protection. There are many similarities among the related themes while examining the writing survey, such as cyberwar admission, digital psychological warfare, and digital attacks (Nam), making it usually difficult to distinguish between them. Despite the similarities in the concepts, using identical approaches results in the categorization, uprightness, and accessibility of data frameworks being lost. According to Hwang et al. (2017), it is essential to develop network safety awareness programs since representatives' ignorance of network security can be seen as obstructing the confidentiality, availability, and integrity of any data framework [10].

A model that illustrates the key goals to achieve data security and data framework security is the Secrecy, Respectability, and Accessibility (CIA) group of three (Figure 1). (Glasser and

Taneja, 2017). The data and data frameworks' assurance is the main focus of the ternion's aims. The security of data frameworks may be determined by a variety of factors, according to Glasser and Taneja. The three most important components of the CIA ternion, namely secrecy, respectability, and accessibility, have, nonetheless, received the most attention. The effective use of data frameworks and related mechanical resources in day-to-day life necessitates the development and implementation of components for protecting data and data frameworks from digital threats and digital attacks [11].

2.6.Economic Influence on Cybersecurity

States have frequently featured the significant expense connected with digital assaults and the administration of weaknesses that do exist and the effect on its data frameworks and organizations. In the Caribbean district, the confidential area has expanded its spending on network safety counteraction strategies, while, the public area has centered its interests on other need regions, like the structure of streets, and has not contributed any critical assets towards alleviating or battling cybercrime [12]. In its Worldwide Network Safety File, the Global Media Transmission Association declared that a cyber-attack can compel the public area to veer off from different debacles to answer and recuperate from a cyber-attack. The first cyber-attack was in 2017 when the Grounds and Studies Division information server in the public area of the Province of Dominica was gone after by ransomware [13]. The Specialized Administrations Division had put more than $500,000 into gathering geospatial data on the area of private and public terrains and had redrawn the current government structures and different structures of critical significance to the Republic of Dominica. This caused a huge effect on crafted by the Specialized Administrations Division since every one of the drawings required for work continuation was deleted. The second cyber-attack happened in 2018 on the web-based installment site of the Inland Income Division of the public authority of Dominica which essentially affected the public authority's income because of clients not having the option to record their duty installments.

Chen and Dongre examined the recuperation cost and financial harms from a cyber-attack. Cyber-attacks incorporate not just the burglary of secret information and data but the lost efficiency, the interruption of the ordinary courses of business tasks, and the loss of notoriety. The Herjavec Gathering in its yearly report expressed that cybercrime will cost the worldwide economy an overabundance of $6 trillion every year by [14]. The distribution of the monetary aftermath of cyber-attacks and data breaks can be one more method for bringing issues to light of representatives to the possible dangers and harms of a cybercrime directed a contextual investigation that zeroed in on the assessed expenses of the lost long periods of work of representatives who were engaged with the digital assaults and the people who needed to deal with the consequences of the double-dealings of the digital assaults and information breaks [15]. In the public area of the Region of Dominica, the deficiency of notoriety might impede the reception of advanced administrations by residents hence diminishing the public authority's capacity to acknowledge future saving through any computerized administrations.

3. CONCLUSIONS

A significant amount of money has been made by digital attacks in poor countries throughout the world by using fraud and online services that prey on human vulnerabilities (SANS, 2019). People have been identified as very probably the most vulnerable group, defenseless against cyber-attacks due to little internet security information and awareness. Thus, the investigation addressed the social issue that the District of Dominica's public assistance and government organization representatives' lack of network security awareness created settings

where digital attacks were harming the data frameworks. To combat any digital threats they may encounter, employees urgently need network safety education and mindfulness. I got the opportunity to demonstrate how designated preparation may have an impact on the level of client awareness and knowledge of network safety by overseeing this study. Online protection is another area of the District of Dominica's public life where a wise plan of action to deal with digital risks and digital attacks has not yet been developed. However, technological advances and a global pandemic continue to fuel the demand for telecommuting and the success of Internet services. The increase in digital attacks reflects the growing reliance on data frameworks and data breakthroughs.

The research contributes to the body of literature and knowledge on client awareness, network protection, and mitigating cyber dangers, including understanding online protection bets. By subjecting representatives to rigorous, in-depth, boring network protection training, this increased level of comprehension may be attained. The review's outcomes demonstrated the level of client awareness and knowledge of network security. The results of this study also helped to break through any barriers that could have existed between the training and the hypothesis. With the use of this information, government organizations are better equipped to address the factors affecting network safety, incorporate online safety into necessary planning, and carry out preparation to achieve a robust network protection atmosphere.

REFERENCES

[1] T. Gibbs, “Seeking economic cyber security: a Middle Eastern example,” *J. Money Laund. Control*, 2020, doi: 10.1108/JMLC-09-2019-0076.

[2] M. J. Pappaterra and F. Flammini, “A review of intelligent cybersecurity with bayesian networks,” in *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, 2019. doi: 10.1109/SMC.2019.8913864.

[3] R. G. Brody, H. U. Chang, and E. S. Schoenberg, “Malware at its worst: death and destruction,” *International Journal of Accounting and Information Management*. 2018. doi: 10.1108/IJAIM-04-2018-0046.

[4] A. P. Singh, G. Sharma, and A. Singh, “A Comparative Study on Modern Password Management,” 2021.

[5] M. Alshaikh, “Developing cybersecurity culture to influence employee behavior: A practice perspective,” *Comput. Secur.*, 2020, doi: 10.1016/j.cose.2020.102003.

[6] A. Saad *et al.*, “Privacy and security gaps in mitigating Cyber crime: The review,” in *2nd International Symposium on Agent, Multi-Agent Systems and Robotics, ISAMSR 2016*, 2017. doi: 10.1109/ISAMSR.2016.7810009.

[7] J. Sebastian, “CYBER TERRORISM: A POTENTIAL THREAT TO GLOBAL SECURITY,” *IEDSR Assoc.*, 2020, doi: 10.46872/pj.84.

[8] P. Chellaiah, B. Nair, K. Achuthan, and S. Diwakar, “Using theme-based narrative construct of images as passwords: Implementation and assessment of remembered sequences,” *Int. J. Online Eng.*, 2017, doi: 10.3991/ijoe.v13i11.7774.

[9] R. Verma and S. Ruj, “Security services using crowdsourcing,” in *Procedia Computer Science*, 2014. doi: 10.1016/j.procs.2014.05.454.

[10] K. Mersinas, T. Sobb, C. Sample, J. Z. Bakdash, and D. Ormrod, "Training Data and Rationality," *Proc. Eur. Conf. Impact Artif. Intell. Robot. (Eciair 2019)*, 2019.

[11] L. Di Martino, "Fear and empathy in international relations: Diplomacy, cyber engagement and Australian foreign policy," *Place Brand. Public Dipl.*, 2021, doi: 10.1057/s41254-021-00211-9.

[12] S. K. Srivastava, S. Das, G. J. Udo, and K. Bagchi, "Determinants of Cybercrime Originating within a Nation: A Cross-country Study," *J. Glob. Inf. Technol. Manag.*, vol. 23, no. 2, pp. 112–137, 2020, doi: 10.1080/1097198X.2020.1752084.

[13] B. Nussbaum and S. Park, "A tough decision made easy? Local government decision-making about contracting for cybersecurity," in *ACM International Conference Proceeding Series*, 2018. doi: 10.1145/3209281.3209368.

[14] D. S. Reveron and J. E. Savage, "Cybersecurity Convergence: Digital Human and National Security," *Orbis*, 2020, doi: 10.1016/j.orbis.2020.08.005.

[15] T. Unwin, "'Cybersecurity' and 'Development,'" in *The Oxford Handbook of Cyber Security*, 2021. doi: 10.1093/oxfordhb/9780198800682.013.59.

CHAPTER 17

IMPORTANCE OF CYBER LAWS AND PREVENTION FOR DATA SECURITY

Ms. Manali Rathore, Assistant Professor,
Seedling School of Law & Governance, Jaipur National University, Jaipur, India,

ABSTRACT:

The term "cyber law" refers to legal concerns relating to the use of communications technology, specifically "cyberspace," or the Internet. The law was passed to protect both individuals and corporations from cybercrime. If someone violates and breaks the law, cyber law enables other individuals or groups to take legal action against that person. Cyber laws protect data from unauthorized access, Internet freedom of speech, privacy, communications, email, websites, intellectual property, hardware, and software, including the data discussed in this paper, and they also help to reduce or deter people from engaging in large-scale cybercriminal activity. Consumers are protected from online fraud by cyber laws. They are meant to prevent internet crimes such as identity and credit card theft. This type of theft carries both federal and state criminal penalties for the offender. Strong cyber security rules and regulations are essential for the future as cyber security is an important concern for the entire planet.

KEYWORDS:

Crime, Cyberspace, Cyber Law, Internet, Security.

1. INTRODUCTION

The idea that the Internet is chaotic and that there should be rules and regulations online seems inconsistent. However, a legal framework known as cyber law exists to regulate cyberspace. Cyber law is a broad term that includes all online laws and regulations. Any company can significantly improve its visibility to millions of people globally by publishing a web page. This aspect of the Internet is the source of much debate in the legal field [1]. Cyber law is a process that is always changing. As the Internet expands, many legal difficulties arise. Cybercrime is one of the most important challenges affecting online today. When the Internet first came into existence, its creators rarely thought that it could potentially be misused for criminal purposes.

These days, there are a lot of unpleasant things occurring online. All actions taken online to commit a crime are referred to as cybercrime. These might either be unlawful actions in the traditional sense or unlawful acts that have arisen as a result of the development of the new medium. People with intellect have been badly abusing this element of the Internet to continue illegal acts in cyberspace because of the anonymity of the Internet, which makes it easy to participate in a range of criminal actions with impunity [2]. The subject of cybercrime

is still developing, and new ways of committing crimes online are becoming more prominent with each passing day.

The invention of the computer has eased human existence; it is now used for a variety of global purposes, from small businesses to large corporations. A computer is a device that can store, utilize, and process data or instructions that have been programmed by a user. Since ancient times, the majority of computer users have used computers for deceptive reasons, either for their gain or the gain of others [3]. This assisted in the development of cybercrime. This has led to gatherings that are outside the law in our culture. Cybercrime is defined as a kind of criminal activity that is often committed online, primarily via the use of mainframes or computer networks. Now, the phrase "cyber law" is used. Although it lacks a fixed definition, we may describe it simply as the law that governs the internet. The laws that govern cyberspace are known as cyberlaws [4]. Cyber Law encompasses topics such as data security and solitude, digital and electronic signatures, and cybercrimes. The first Information Technology Act of India was proposed by the UN General Assembly and was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model.

The Internet is a network of linked, globally distributed computer systems that use the Internet Protocol Suite (TCP/IP). It is a network of networks composed of millions of academic, commercial, government, and private networks, ranging from local to global reach, that are connected via copper lines, fiber-optic cables, wireless connections, and other technologies [5]. The World Wide Web (WWW) and the infrastructure that supports electronic mail are two of the many information resources and services available on the Internet. Other well-known services include online chat, file transfer and sharing, online gaming, and Voice over Internet Protocol (VoIP), which enables voice and video communication between two people.

The United States financed research efforts by its military agencies to create reliable, fault-tolerant, and dispersed computer networks in the 1960s, when the Internet first emerged. This research resulted in the commercialization of an international network in the mid-1990s and a new U.S. project by the National Science Foundation. In common parlance, the terms Internet and World Wide Web are often used interchangeably [6]. However, the World Wide Web and the Internet are not the same thing. A worldwide system for data transmission is the Internet. The infrastructure that connects a computer is made up of both hardware and software components. On the other hand, the web is one of the services provided through the internet. It is a set of related files and other resources linked through hyperlinks and Uniform Resource Locators (URLs).

In today's era of exponential growth, information technology permeates every aspect of society. The switch from document-based to paperless communication is now achievable thanks to technological advancements. To drive innovation, creativity, and general productivity, we are now developing new communication principles that emphasize speed, efficiency, and accuracy. Computers are often used to store sensitive information of political, social, economic, or delicate nature, to greatly benefit society [7]. The rapid worldwide expansion of computer and Internet technologies has increased Internet-related crimes.

These crimes know almost no boundaries and can harm any nation on the planet. So there is a need for awareness and mandatory rules to prevent computer-related crime in all countries. Internet- and computer-based trade and communications operate on a global scale regardless of defensive barriers, opening up a new sphere of human activity and challenging the viability and legality of enforcing laws based on geographic boundaries [8]. Screens and passwords, which make up the new peripheral, divide the "cyber world" from the "real

world" of atoms. The authorities responsible for enforcing and making laws on a regional basis consider this new environment to be very dangerous.

1.1.Need for Cyber Law:

When the internet was first created, its creators barely imagined that it would grow into a pervasive revolution that would demand regulation since it might be used for illegal purposes. These days, there are a lot of unpleasant things occurring online [9]. People with intellect have been badly abusing this element of the internet to continue illegal actions in cyberspace because of the mysterious character of the internet, which makes it possible to participate in a range of crimes with impunity.

1.2.Importance of Cyber Law:

Because it affects practically every element of transactions and activities using the internet, the World Wide Web, and cyberspace, cyber law is significant. At first glance, it could seem that cyber laws are a highly technical area and have nothing to do with the majority of online activity [10]. Whether we are aware of it or not, every action and response in cyberspace is influenced by legal and ethical considerations. It is crucial to recognize the negative effects of the internet and put a stop to cybercrime. Every action you do in cyberspace may and will be viewed from a legal viewpoint since the Internet is evolving and is now thought of as the best medium to have ever existed in human history. There are different cyber legal problems present at every stage, from the moment you register your domain to the time you put up your website to the time you perform electronic commerce on the same site. These problems may not affect you now since you believe they do not affect your online activity [11]. However, you will eventually need to cut costs and pay attention to cyber legislation for your profit.

Cyberlaw is always changing and evolving. Because it is a process that is continually changing, cyber law is appropriately adapting to meet the demands of the times as new possibilities and problems emerge. As the internet expands, several legal difficulties arise. Domain names, intellectual property rights, electronic commerce, privacy, encystations, electronic contracts, cybercrime, online banking, spamming, and other difficulties are among them. It's a lengthy list. Every time a cybercrime advances and a cybercriminal's thinking is evaluated to commit a cybercrime, the cyberlaw is also evaluated to stop the crime. Today, there is a growing understanding of cyber law. At first, a lot of technical specialists held the opinion that legislative control is not required. However, given the fast advancement of technology and the internet, it is obvious that no online action can escape the reach of cyber law. Any commercial firm or entity may greatly boost its visibility to millions of people, organizations, and governments worldwide by publishing a Web website. That aspect of the internet is the one that has the legal community divided.

2. DISCUSSION

Since the advent of computers, it has been simpler for people to utilize them for a variety of tasks. Small and big businesses alike depend on computers and Internet services for their work, transactions, and paperwork. Computers are utilized nowadays all around the globe, and as we all know, everything has its benefits and drawbacks. Cybercrime is the main issue that develops with technology and computers [12]. Data interpretation and phishing are a few examples of cybercrimes. Different cyber laws are being created to restrict these crimes to protect organizations from becoming victims. The rules that govern the internet are known as cyber laws. To regulate cybercrimes, several cyberlaws that provide facilities like digital signatures and data encryptions are currently being implemented.

With the development of cyber technology, the German State of Hesse passed the "Data Protection Act, of 1970," which is considered to be the first computer-specific regulation in the world. Since then, all online action in India and throughout the world is governed by cyber laws.

The legislation governing information technology, including computers and the internet, is known as cyber law or IT law [13]. It oversees the digital distribution of information, software, information security, and e-commerce.

It is connected to legal informatics. IT law encompasses elements of contract, intellectual property, privacy, and data protection laws rather than being a distinct field of law. A crucial component of IT law is intellectual property. In Europe and other parts of the world, the subject of software licenses is contentious and still developing.

2.1. Area of Cyber Law:

Cyber laws serve a variety of functions. Some laws provide guidelines for how people and businesses can use computers and the Internet, while others protect citizens from becoming victims of crime as a result of dishonest online activity [14]. The major domains of cyber law are:

2.1.1. *Fraud*: Cyber laws are essential to consumers' protection against online fraud. Legislation is created to stop online financial crimes including credit card fraud, identity theft, and others. Identity thieves may be charged as accomplices or as state criminals. They could also run into a victim-driven civil lawsuit. Cyber attorneys strive to both defend and prosecute clients accused of online fraud.

2.1.2. *Copyright*: Internet use has made it simpler to violate copyright laws. When people first started communicating online, copyright infringement was all too common. To bring a lawsuit to impose copyright protections, both businesses and individuals require attorneys. The field of cyber law known as copyright infringement defends people's and businesses' legal entitlements to financial gain from their creative works.

2.1.3. *Defamation*: Many employees utilize the Internet to voice their opinions. It may cross the line into defamation when individuals use the internet to spread false information. Civil rules called defamation laws protect people from false public remarks that might damage their reputations or those of their employers. Defamation legislation is used when persons post remarks on the internet that are illegal under civil laws.

2.1.4. *Harassment and Stalking*: Online comments might sometimes be unlawful under the criminal laws that prohibit stalking and harassment. Both civil and criminal laws are broken when someone repeatedly posts threatening comments about another individual online. When stalking happens via the internet or through another electronic contact, cyber attorneys both prosecute and defend the victim.

2.1.5. *Freedom of Speech*: The right to free expression is a crucial component of cyber law. Cyber laws prohibit some online acts, yet free speech rules also permit individuals to express their opinions. Cyber attorneys must inform their clients of the restrictions on free expressions, such as those relating to laws against obscenity. When there is a disagreement over whether a client's acts qualify as legal free speech, cyber attorneys may also stand up for them.

2.1.6. Trade Secrets: Cyber laws are often used by businesses doing online transactions to safeguard their trade secrets. For instance, the algorithms used by Google and other Internet search engines to generate search results are developed over a long period. They also devote a lot of work to creating additional features, like search services for flights, intelligent help, and maps. Cyber laws assist these businesses in pursuing legal action when required to safeguard their trade secrets.

2.1.7. Contracts and Employment Law: You have violated cyber law each time you click a button that indicates your agreement to a website's terms and conditions. Every website has terms and conditions that are somewhat connected to privacy issues [15].

When it comes to cybercrime, online abuse, etc., cyber law is essential. Today's high-tech age has led to certain individuals exploiting the internet for numerous illegal activities including online scams and hacking, among others. Cybercrime refers to these illicit internet-related acts. The Government of India enacted the Cyber Law to curb cybercrimes and penalize those responsible [16].

The problem of online abuse is governed by cyber law. Cyberlaw, which deals with issues connected to the Internet and cybercrime, is referred to as the "law of the internet." This law's main goal is to stop different cybercriminal behaviors.

People and organizations who utilize the Internet for business and professional reasons are legally protected by cyber law [17]. It safeguards communications, privacy, and information access while using the internet, websites, software, etc.

Electronic papers are given legal significance under cyber law. Making legislation similar to a cyber law is important given the ongoing increase in crimes in India. The Information Technology Act, of 2000, which went into effect on October 17, 2000, contains provisions for cyberlaw in India [18].

The Internet is used as a research and information-sharing tool in today's tech-savvy atmosphere [19]. Cybercrimes are created as a result of the growing number of internet users.

Cyber Law handles all concerns about cybercrime or digital crime. Therefore, the necessity for cyber law develops to get a remedy against cybercrime. In a nation like India where the internet is widely utilized, cyber legislation is crucial [20]. The legislation was passed to protect individuals and institutions against cybercrime and other crimes connected to the internet.

It safeguards the privacy of each person and company. There was no explicit legislation in India dealing with cybercrime before the adoption of Cyberlaw. A person who conducts cybercrime is subject to penalty under the Cyber law's norms and regulations [21].

Someone else or an organization can take legal action against someone who disobeys and breaches the law.

2.2.The advantages of Cyberlaw:

Stopping cybercrimes is the main goal of cyber law. However, there are certain benefits to cyber law, some of which are shown in Figure 1:

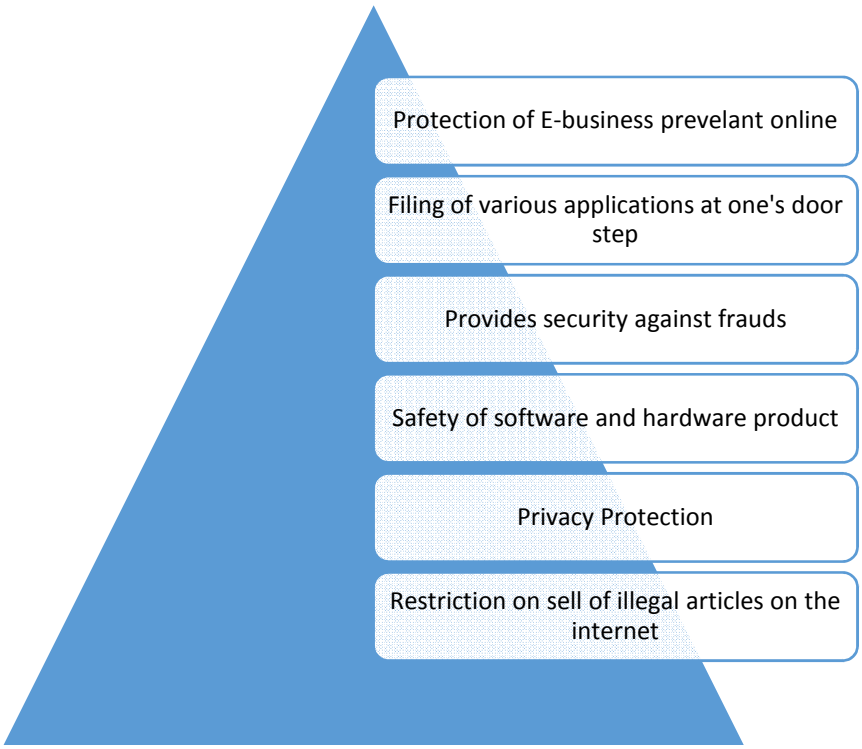

Figure 1: Illustrate the advantages of cyber law for different roles.

2.3.The regulatory framework of Cyber Law:

The Information Technology Act, of 2000 was established by Parliament to provide a legal framework for e-commerce in India. The Information Technology Act, of 2000, sometimes referred to as Cyber Law, is currently the supreme law of India. The Acts, Rules, and Regulations listed below are part of the cyber laws shown in Figure 2.

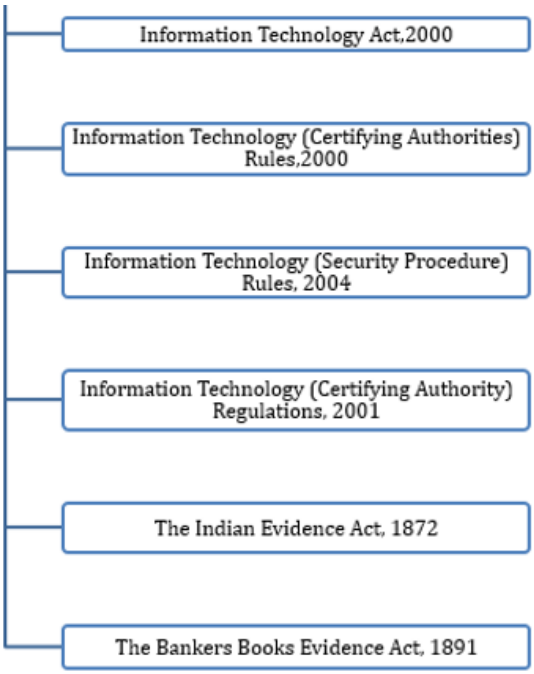

Figure 2:Illustrate the cyber law for IT security proposed.

The conclusion that computer-related crime is a real, expanding occurrence may consequently be harmful. Additionally, a consistent increase in these crimes is anticipated in this area, which calls for increased attention from politicians. Further research and in-depth analysis will be required, and improper use of the Internet will be a liability [22]. The urgent requirement of the hour is for strict and austere rules to be created and honestly applied. Individual users choosing to join the specific systems they find most enjoyable may, in our opinion, help the law of the Internet continue to evolve [23]. The criminal activity of the various age groups has been shown through general statistics. In this new dynamic framework, which must be enforced and anticipates shedding light on the usefulness of cybercrime, we must rethink cyber-legal procedures [24]. Last but not least, the Cyber Law, which is a mindful discussion among group members about fundamental principles and specific societal advantages, will endure. This paper's perspective focus is on preventing cybercrime across various age groups by emphasizing the psychological aspects of human-created cybercrime and ensuring new and updated versions of cyberlaws, both of which are urgently necessary to address the issue shown in Figure 3.

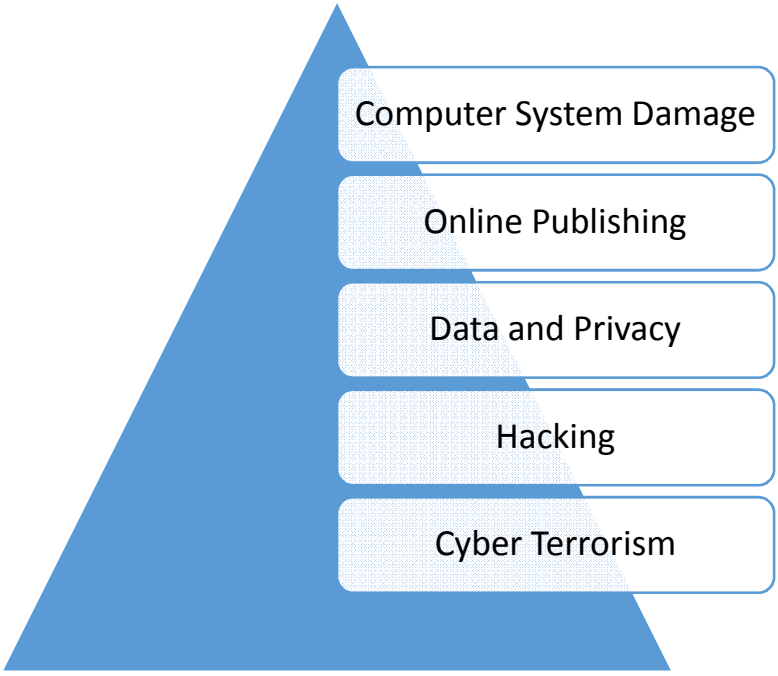

Figure 3: Illustrate major areas of cybercrimes covered under the Indian IT Act.

The area of the legal system that deals with legal informatics and regulates e-commerce, software, and information security is known as cyber law, commonly referred to as Internet law or cyber law. It is connected to electronic components including computers, software, hardware, and information systems as well as legal informatics [25]. It covers a wide range of issues, including online privacy and freedom of speech, as well as how to access and use the Internet. Cyber laws protect information from unauthorized access, and freedom of speech related to Internet use, privacy, communications, email, websites, intellectual property, hardware, and software, such as data storage devices, and they also help to reduce or stop people from engaging in large-scale cybercriminal activities.

Globally, there are more legal difficulties as a result of the Internet's daily, fast traffic growth. Cyber laws vary by nation and territory, with reparation ranging from penalties to jail with enforcement being difficult. For anyone who uses the Internet or operates an online company,

cyber law provides legal rights [26]. Internet users must be aware of their country's cyberlaw and local laws to determine what actions are permitted or prohibited on the network. They may also shield us from unapproved actions. The first cyber legislation, known as CFFA and passed in 1986, was the Computer Fraud and Abuse Act. This legislation helped to guard against unauthorized access to computers. Additionally, it described the many levels of punishment for violating that legislation or engaging in any criminal behavior, as seen in Figure 4.

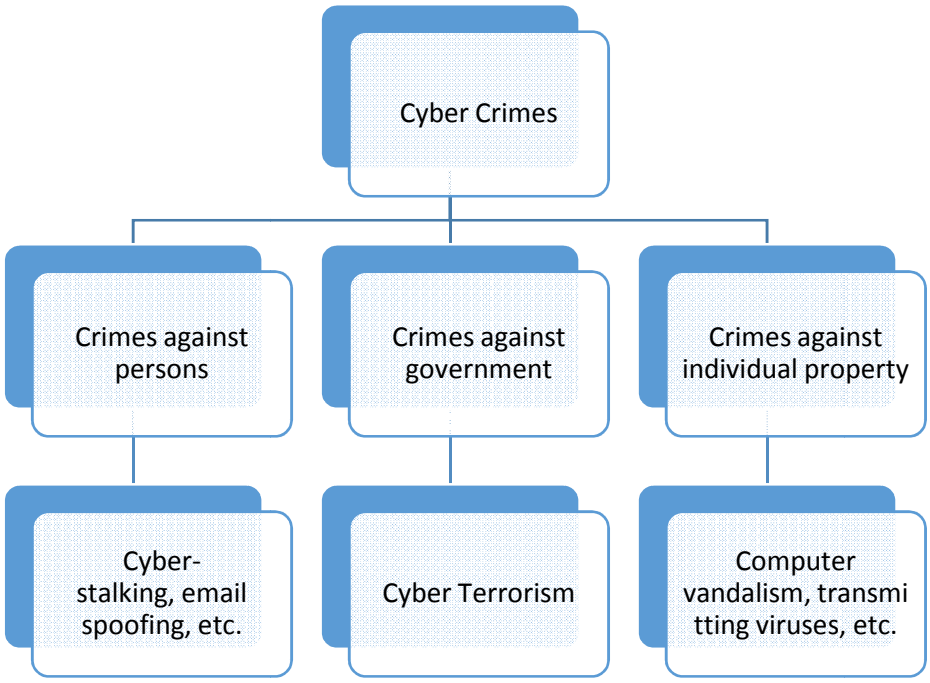

Figure 4:Illustrate cybercrimes in different levels of persons, government, and individuals.

A new area of law is called cyber security law. In our everyday lives, cyber security is essential. Any crime done utilizing technology is prohibited under Indian cyber laws. The network may be hacked into to get allowed access, or a computer can be contaminated to introduce a virus into the application. Cyberspace is the name given to our computer-generated internet universe, and cyber laws refer to the regulations that apply there. Laws about internet information technology are known as "cyber laws."

Cyberspace includes conventional crimes including theft, fraud, forgery, and defamation. When we discuss cyberspace in this context, we must recognize that it is an infinite medium. Because it covers all facets of online transactions and activities on the World Wide Web and in cyberspace, cyber law is significant. Cybercrime and cyber security are closely related. Cybercrime is the term for crimes committed using computers and the internet.

3. CONCLUSION

As is common knowledge, most things in this day and age are done online, from online large businesses to online transactions. Anyone may access internet resources from wherever making the web a worldwide platform in the meanwhile. Only a select few individuals have used internet technology for unlawful activities including swindles and unauthorized access to other people's networks. Cybercrime is the term used to describe these criminal offenses or crimes committed online. The phrase "cyber law" was popularized to stop or punish

cybercriminals. Cyber law is a subset of legal procedures that deals with the Internet, the World Wide Web, and legal matters. It covers a broad range of themes, including freedom of speech, access to and usage of the Internet, and online security or privacy. It is often referred to as the "law of the web".

REFERENCES

[1] S. Mehta and V. Singh, "a Study of Awareness About Cyberlaws in the Indian Society," *Int. J. Comput. Bus. Res.*, vol. 4, no. 1, 2013.

[2] M. A. Pitchan and S. Z. Omar, "Cyber security policy: Review on netizen awareness and laws," *J. Komun. Malaysian J. Commun.*, 2019, doi: 10.17576/JKMJC-2019-3501-08.

[3] C. Mambile and P. E. Mbogoro, "Cybercrimes awareness, cyber laws and its practice in public sector tanzania," *International Journal of Advanced Technology and Engineering Exploration*. 2020. doi: 10.19101/IJATEE.2020.762051.

[4] A. Sarmah, R. Sarmah, and A. J. Baruah, "A brief study on Cyber Crime and Cyber Law ' s of India," *Int. Res. J. Eng. Technol.*, 2017.

[5] J. H. Awan, S. Memon, and F. M. Burfat, "Role of cyber law and mitigation strategies in perspective of Pakistan to cope cyber threats," *Int. J. Cyber Warf. Terror.*, 2019, doi: 10.4018/IJCWT.2019040103.

[6] S. Rackevičienė and L. Mockienė, "Cyber Law Terminology as a New Lexical Field in Legal Discourse," *Int. J. Semiot. Law*, 2020, doi: 10.1007/s11196-020-09690-0.

[7] M. Parasol, "The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams," *Comput. Law Secur. Rev.*, 2018, doi: 10.1016/j.clsr.2017.05.022.

[8] S. D. Jayasekara and I. Abeysekara, "Digital forensics and evolving cyber law: case of BIMSTEC countries," *J. Money Laund. Control*, 2019, doi: 10.1108/JMLC-02-2019-0019.

[9] M. N. Simović, Ž. Rašević, and V. M. Simović, "CYBER WARFARE AND INTERNATIONAL CYBER LAW: WHITHER?," *J. Criminol. Crim. Law*, 2020, doi: 10.47152/rkkp.58.3.2.

[10] R. M. Kamble, "Cyber Law and Information Technology," *Int. J. Sci. Eng. Res.*, 2013.

[11] K. R. R. Bhatele, D. D. Mishra, H. Bhatt, and K. Das, "The Fundamentals of Digital Forensics and Cyber Law," in *Cyber Warfare and Terrorism*, 2020. doi: 10.4018/978-1-7998-2466-4.ch005.

[12] B. Sahu, S. K. Sahu, N. Sahu, and P. Sahu, "Identify uncertainty of cyber crime and cyber laws," 2013. doi: 10.1109/CSNT.2013.100.

[13] O. A. Hathaway *et al.*, "The law of cyber-attack," *California Law Review*. 2012.

[14] K. E. Eichensehr, "The cyber-law of nations," *Georgetown Law Journal*. 2014.

[15] A. Lubin, "Cyber law and espionage law as communicating vessels," 2018. doi: 10.23919/CYCON.2018.8405018.

[16] Y. Sufriadi, “Prevention Efforts Against E-Commerce Fraud Based on Indonesian Cyber Law,” 2021. doi: 10.1109/CITSM52892.2021.9588900.

[17] S. Bhattacharya, B. KaurSachdev, and, A. Kundu, “Impact of Cyber Law in Modern Era With Advancement in Technology and Protection From Rising Threats of Cyber Crimes in Our Socio Economic Sector,” *Int. J. Adv. Res.*, 2021, doi: 10.21474/ijar01/13404.

[18] S. Khan and P. M. Tehrani, “Examination of restriction of free speech under international covenant on civil and political rights (ICCPR) in reference to prevention of electronic crimes act 2016, Pakistan,” *Int. J. Recent Technol. Eng.*, 2019, doi: 10.35940/ijrte.B1084.0982S919.

[19] E. F. G. Ajayi, “Challenges to enforcement of cyber-crimes laws and policy,” *J. Internet Inf. Syst.*, 2016, doi: 10.5897/jiis2015.0089.

[20] M. I. Ali and S. Kaur, “The Impact of India’s Cyber Security Law and Cyber Forensic on Building Techno-Centric Smartcity IoT Environment,” 2021. doi: 10.1109/ICCCIS51004.2021.9397243.

[21] B. E. Cartwright, “Cyberbullying and cyber law,” 2016. doi: 10.1109/ICCCF.2016.7740430.

[22] M. Singh, J. Husain, and N. Vishwas, “A Comprehensive Study of Cyber Law and Cyber Crimes,” *Int. J. IT, Eng. Appl. Sci. Res. I*, 2014.

[23] H. Younies and T. N. el Al-Tawil, “Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE),” *J. Financ. Crime*, 2020, doi: 10.1108/JFC-04-2020-0055.

[24] I. Sharma and M. Afshar, “Privacy and Freedom Issues in Cyberspace with Reference to Cyber Law,” *Int. J. Comput. Appl.*, 2016, doi: 10.5120/ijca2016910185.

[25] Z. Sattar, S. Riaz, Shafia, and A. U. Mian, “Challenges of cybercrimes to implementation of legal framework,” 2019. doi: 10.1109/ICET.2018.8603645.

[26] A. Shahzad, “Cyber-Terrorism Law, Implementation and Ways Forward,” *Int. J. Electron. Crime Investig.*, 2019, doi: 10.54692/ijeci.2019.030232.

CHAPTER 18

A BRIEF INVESTIGATION TO TRADEMARK AND COPYRIGHT IN PATENT SECURITY

Ms. Poojyashree Kumawat, Assistant Professor,
Seedling School of Law & Governance, Jaipur National University, Jaipur, India,
Email Id-poojyashree.kumawat@jnujaipur.ac.in

ABSTRACT:

A trademark is a term, symbol, pattern, or phrase used to identify a particular product and set it apart from competing goods. The phrase "original works of copyright" refers to things like literature, works of art, music, and architecture. The main objective of copyright and trademark is to new ideas, procedures, or scientific discoveries are protected by patents; brands, logos, and catchphrases are protected by trademarks; and original literary works are protected by copyrights. A trademark remains active as long as it is being used; in contrast, copyright expires after one predetermined amount of time. In conclusion, if these two intellectual property protections apply to your company, they may be helpful. Protection for an enterprise's business is provided by trademark registration. The range of protection is fairly broad because it covers both similar and identical trademarks. Many nations provide additional privileges to well-known trademarks.

KEYWORDS:

Copyright,Patent Security, Trademark,World Trade Organizations.

1. INTRODUCTION

Intellectual property rights enable individuals to establish ownership rights over the outcomes of their creative and innovative operations in the same way that physical property allows them to. Because intellectual property is created by human labor, it is a multiple that is subject to change. Patents, brand names, designs, and copyrights are the four main types of property rights. This article will cover trademark law, which is a crucial aspect of imp rights. Trademarks in India are statutorily protected under the Trademark Act, of 1999, as well as under the common law remedy of passing off. The Controller General of Patents, Designs, and Trade Marks is a government agency that reports to the Department of Industrial Affairs and Promotion (DIPP), which is part of the Ministry of Commerce and Industry. It also addresses the rights of the trademark holder, penalties for infringement, treatments for damage, and modes of trademark transference.

The trademark law addresses the registration mechanism, trademark protection, and the prevention of fraudulent trademarks. The trademark law also addresses the rights obtained through trademark registration, modes of transfer and assignment of rights, the nature of infringements, sanctions for such infringement, and remedies available to the owner in the event of such infringement. The Trademark Act of 1999 defines a trademark as "a mark capable of being represented graphically and capable of differentiating the goods or services provided by one individual from those of others, and may include the shape of goods, their

packaging, and combination of colors." Such a mark could include signatures, names, labels, headings, and so on.

A trademark is a term, sign, symbol, smartphone, brand, planning to head, label, ticket, name, letter, word, handwritten note, numeral, the shape of goods, packaging, or color combination, or any such combination or even a graphic that is used to distinguish a company, its products, or services from those of its competitors. A brand, product, company name, or logo, for example. Customers can then choose, buy, and enjoy goods and services according to the particular qualities and attributes that the trademark's owner/user has promised. The trademark prevents the unauthorized use of an individual's or company's product or service.A trademark can consist of logos, images, words, simple sentences, colors, or a combination of all of these. Words and images are the most common, but other distinguishing symbols may be used if they can be represented graphically.

The legal right of the proprietor of intellectual property is referred to as copyright. Simply put, copyright refers to the license to copy. This means that the only people who have the unique right to reproduce the work are the original creators of the products and anyone they give permission. Copyright law grants original material creators the exclusive right to further use and duplicate that content for a set period, after which the copyrighted item becomes public domain

A patent is a kind of trademark that grants the owner the legal right to prevent others from attempting to make, use, or sell an invention for a limited time in exchange for the publication of an enabling disclosure of the invention. In most countries, patent applications are governed by private law, and the patent owner must sue someone who infringes on the patent to enforce their rights. Patents are an important source of competitive advantage in some industries, but not in others.

According to national laws and international agreements, the procedure for granting patents, the prerequisites placed on the patentee, and the extent of the exclusive rights vary greatly between countries. A patent application, on the other hand, must typically include one or more claims that describe the scope of protection sought. A patent may contain numerous claims, every one of which defines a distinct property right.

According to the World Trade Organization's (WTO) TRIPS Agreement, patents should be obtainable in countries that are members of the WTO for any invention, in any field of technology, as long as it is new, involves an inventive step, and is capable of industrial application. Nonetheless, there are differences in what constitutes a patentable subject from region to region, as well as among WTO member states. TRIPS also requires that the duration of available protection be at least twenty years.

2. LITERATURE REVIEW

Nikolaos Alexiou [1] et al. explained international licensing revisited: the role of copyright and trademark enforcement strength which - The goal of this paper is to investigate the role of copyright and trademark regulation strength in stimulating licensing flows in 21 countries. Design/methodology/approach - In doing so, panel data methodology serves as the empirical platform for the investigation of the trademark and copyright regulation strength levels of 21 countries and the choice between unregistered and affiliated licensing of US firms from 1998 to 2011. Findings - The evidence suggests that the strength of copyright and trademark enforcement has a highly significant effect on licensing and that higher levels of regulation stimulate higher levels of unregistered licensing. Originality/value - The authors employ two

longitudinal indices of copyright and trademark enforcement strength in 21 countries to evaluate both the efficacy and efficiency with which copyrights and trademarks are enforced.

Tammenlehto, Laura [2] et al. discussed copyright and trademark crimes in the Nordic countries: analysis from the perspective of the principle of legality In the Nordic countries, the principle of legality limits criminalization. The purpose of the theory is to uphold this same legitimacy of the state's penal authority and to protect an accused's rights by guaranteeing the clarity and predictability of the criminal law. The Nordic IPR crime clauses are extensive, but it is difficult to determine the limits of criminalization based on them. Multiple internal references and just a blanket criminalization technique, combined with inaccurate definitions of objects of protection, are particularly problematic elements of this legislation. Three problematic aspects of copyright and trademark are addressed: the copyrighted task thre shold ethical theories, and trademark establishment through use.

Gusti Ngurah Marwanto [3] et al. explained A character created or depicted in an interactive story to support the story in an animated film is known as an animated cartoon character. Many baby clothes, bags, shoes, and accessories now include animated images from cartoons to attract buyers' attention and increase the revenues of these products. The goal of this writing is to identify, analyze, and extravagant legal protections for animated cartoons based on copyright law provisions, as well as protection under the law for animated cartoon characters, used as brands. Normative legal research was conducted using statutory, conceptual, and analytical approaches. Animated cartoon characters, as one of the objects of copyright protection, namely images, are automatically protected under the Copyright Act and can also be registered as Trademarks, as hard as the image has distinctive power and no substantial or entire similarity.

Link, Albert N.van and Hasselt, Martijn the use of intellectual property protection mechanisms by publicly supported firms in which Intellectual property protection mechanisms (IPPMs) are used by technology firms to appropriate the returns on their research investments. The empirical literature has generally focused on private sector firms' use of IPPMs to appropriate the results to their privately financed R&D-based technology solutions. Until now, studies haven't considered the utilization of IPPMs by companies in the private sector whose research is funded by the government. Using a portfolio of formal IPPMs comprised of patents, copyright holders, and trademarks, we empirically identify a few important covariates.

Graham, S. and Somaya, D. [4] explained complementary uses of patents, copyrights, and trademarks by software firms: evidence from litigation To investigate the concurrent and intersecting IP protections used by software firms, we used litigation data on patent rights, copyrights, and trademarks. Despite the relative lessening of legal copyright protection in the 1990s, we find that software firms have a remarkably large and growing reliance on copyright enforcement. While previous research and policy debate has tended to view different types of intellectual property as substitutes, we propose prerequisites under which they're able to act as complements.

Bhat, S. Ravindra [5] explained innovation and intellectual property rights law in an overview of Indian law In India, specific legislation enacted by the Parliament addresses the many aspects of intellectual property rights. These laws operate within the Indian Constitution's overarching warranty of property right. While providing brief overviews of the law of patent rights, copyrights, trademarks, and designs, as well as remedies for violations of these rights, the article also addresses issues concerning the intersection of these rights in

practice. The article also refers to highly influential judicial decisions in these areas of law where appropriate.

Zekos, Georgios I [6] explained the influence of patents, copyright, trademarks, and competition on GDP, GDP growth, trade, and FDI which is Foreign Direct Investment (FDI) is the process of creating or acquiring a subsidiary in which the venture capitalist has extensive management control. It can include capital, technology, or some intangible advantage. The empirical results demonstrate the impact of patents, copyright, trademarks, and competition on GDP and GDP growth, which varies depending on the explanatory variables used in our econometric models. Given that IPRs contribute to an economy's competitiveness, there is an interaction between competition and IPR, as well as a complex influence of both factors on FDI inflows, GDP, GDP growth, and trade.

Patel, Pankaj C., and Pearce, John A. [7] explained the survival consequences of intellectual property for retail ventures While the value of patents is widely documented for technology ventures, whether retail expeditions can benefit from patents, copyrights, or trademarks remains unexplored. Given retail ventures' lower survival rate, whether investing in intellectual property can improve their chances of survival is an important research question for both the retailing and entrepreneurial spirit literature. Retail ventures have a lower chance of survival, according to the Kauffman Firm Survey, which included 585 retail and 2406 non-retail ventures. Patents, trademarks, or copyrights in retail ventures increase the odds of survival when compared to non-retail ventures. The findings have implications for intellectual property resource allocation in retail ventures.

Trina Paranjpe, [8] et al. discussed Intellectual property (IP) refers to a variety of distinct types of intangible assets. IP protection enables a rightsholder to prevent others from interfering with or making use of a property right in a specific way. Patents, copyrights, trademarks, and trade secrets are the most common types of intellectual property. Each type of IP protection is unique, with differences in the particular topic that can be protected, the timeframe for protection, and the total cost. Although some inventions may be protected by multiple types of intellectual property, it is critical to consider a variety of business and legal factors before deciding on the best protection strategy. Some technologies necessitate strong intellectual property protection to be commercialized, but unnecessary costs can stymie a product's release. Organizational IP departments weigh these considerations and perform critical IP protection functions. This primer introduces scientists to the various types of intellectual property and their legal implications.

3. DISCUSSION

3.1 importance of patent:

Patents benefit society because they encourage innovation and the development of new products. They also safeguard intellectual property. When an inventor receives a patent, they safeguard the right to exclude others from using, making, and selling one‘s product or method of use for 20 years, while retaining the exclusive and higher-priced right to sell the item.Patents are valuable assets that allow inventors to make public their inventions without fear of infringement. Furthermore, it accelerates the country's growth and development by making advances available to the scientific establishment. A patent, on the other hand, will be granted only if it meets the conditions for patentability. The goal of a patent is to grant an inventor(s) the right to prevent others from exploiting the invention. As a result, anyone other than the inventor is not permitted to use, manufacture, or sell a patented invention even without the inventor's permission. This is commonly referred to as the invention's exclusive right. The investor can profit from this exclusive privilege and commercialize his patent.

The term patent refers to the right bestowed to any individual who invents anything new, useful, and non-obvious. A patent is frequently referred to as a type of intellectual property right, an expression that also refers to trademarks as well as copyrights and has supporters and detractors Other types of intellectual property rights are also referred to as patents in some jurisdictions: industrial design rights are known as design patents in the United States, plant breeders' rights are known as plant patents, and utility models and Gebrauchsmuste are known as petty patents or innovation patents.The additional qualification utility patent is sometimes used to distinguish the primary meaning from these additional types of patents (primarily in the United States). Biological patent rights, business method patents, chemical patents, and software patents are examples of invention patents.

3.2 Importance of trademarks

A trademark is a kind of intellectual property that consists of a recognizable sign, design, or expression that differentiates the products or services of one source from those of others. Service marks, also known as brand names, are commonly used to identify services. A trademark can be possessed by a person, a business organization, or any legal entity. A trademark can be ended up finding on a package, label, voucher, product, or company property. In other words, trademarks identify a specific entity as the supplier of goods or services.

A good trademark should be simple to say and remember while still retaining its distinctiveness and uniqueness. The Brand Value and reputation of a Brand Name heavily influence a consumer's decision to purchase goods or hire services. Because it discourages competitors from using similar names or logos, it is a valuable intellectual asset for a company. In addition, our Legalraasta team helps with trademark registration as well as allows your customers to associate visual cues with your products, fostering customer loyalty.

The owner has the sole right to use the mark for all products that fall into the applicable class(es). Furthermore, the owner owns the Trademark and has the authority to prevent others from using it in the same class where it has been registered. It gives the owner of the registered trademark the option of suing the unauthorized user. In other words, the proprietor owns the trademark and has the authority to prevent others from employing it within the class(es) in which it is registered. It also empowers the owner to sue for any unauthorized infringement.

Registration of Global Trademarks: Don't be concerned if you want to expand beyond India or simply register a trademark in another country; a trademark that was previously registered in India can serve as a solid foundation for gaining worldwide support. A trademark that has already been registered in India can serve as the basis for registration in another country because of all the goodwill accumulated. In other words, a registered trademark in India blended with established goodwill inside the country can provide a solid foundation.

Every entrepreneur must ensure that his or her brand is protected from competition. If the individual's trademark has already been registered by someone else, the individual not only loses business and goodwill in the economy but also loses the ability to prevent others from using the same trademark. As a result of shielding the trademark, the business will be protected, which will benefit the individual by preventing others from employing a similar trademark.

The registration of a trademark creates an intangible asset in a company's balance sheet, namely Intellectual Property, which provides all of the benefits associated with so assets. A registered trademark is a created right that can be sold, designated, franchised, commercially

contracted, converted or purchased, or even used as collateral to obtain a loan. A trademark registration is a valuable asset that generates direct goodwill for a company, brand, or business. We are all aware that the worth and reputation of a trademark have a significant impact on a consumer's willingness to buy a product or service. If that isn't reason enough to get your brand image trademarked right away, Legalraasta can help.

Builds trust and loyalty, as well as goodwill: The significance of trademark registration reflects a product's or service's reputation and excellence. Registering a trademark boosts customer confidence and market recognition. The established performance of your product and services is known to everybody via your trademark, which builds market trust and goodwill. It contributes to the development of loyal customers who always choose the same brand as well as long-term clients who prefer your trademarked brand over others.

Product differentiation helps customers find your products, distinguishes them from established and anticipated competitors and serves as an effective service software. The logo can communicate the vision, quality, or distinguishing features of your company or organization. It sets your product or service apart from the competition while also serving as an effective marketing device. Furthermore, your trademark or logo symbolizes the vision, quality, and uniqueness of the organization. Figure 1 shows the copyright, trademark, and patent relations.

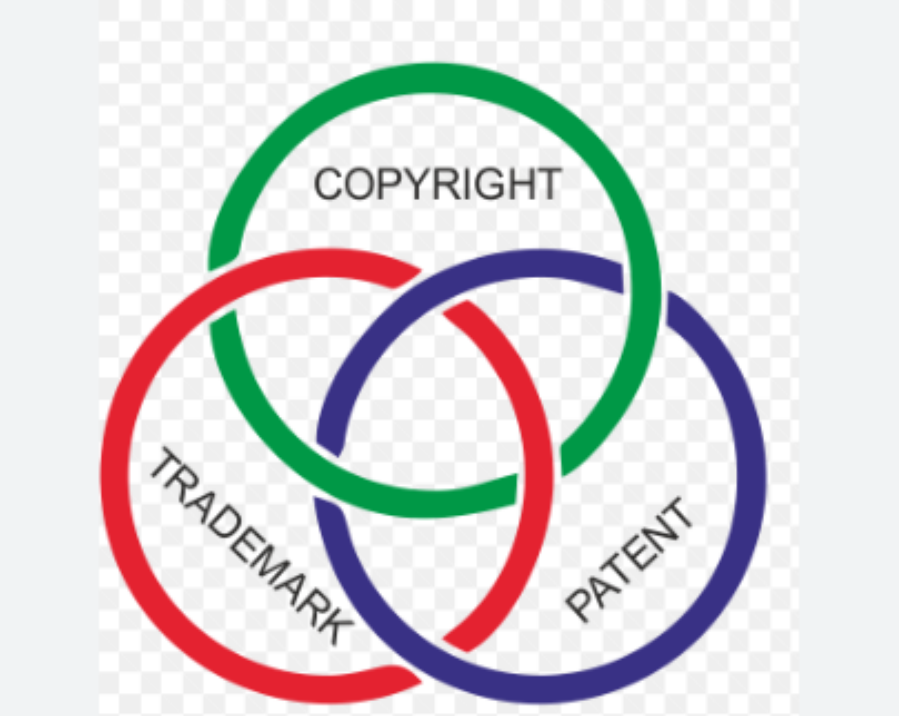

Figure 1: Represent the copyright, trademark, and patent relations

Customers associate the quality of a product with the brand name, and an image of the quality of a specific brand is formed in the market, which aids in drawing in fresh consumers because they can differentiate the quality of a product by logo or brand name. The registration of a trademark provides tangible proof of the value and worth of your business or good. Customers associate a trademark with the quality of a service or product. Obtain an exclusive trademark registration for the brand to attract customers and stand out, and as a result, build its prestige over it.

3.3 Procedure for Copyright Registration:

Copyrights apply to everything you create, and some of them seem to be copyrighted for movies, pictures, journals, music, and so on. Copyright protection is recommended to protect your work. Here are some examples of the significance of copyright:

1. ideas are copyrighted, they can be published to the public, establishing ownership.
2. work is copyrighted, can protect it, and sue for damages in the event of infringement.
3. The owners will be able to keep a record of the enrollment with Indian Customs and avoid importing duplicate copies.
4. The original registered work can be used to create any work that is based on another work that may be subject to copyright restrictions.
5. work or ideas may be sold or shared with such a third party without objection.
6. work is protected by copyright; you may exhibit it.

A copyright is a monopoly granted to the owner of intellectual property. Copyrights safeguard a creator's work against unauthorized duplication or use. Nobody can copy, imitate, or start producing another work if it is protected by Copyright Registration, according to the Copyright Public Performance. This article discusses the significance of copyright.

3.4 Types of patents:

This is what most people envision when they consider a patent. It is a lengthy technical document that instructs the general public on how to use a new machine, method, or system. Congress defines the types of inventions that are protected by utility patents. New technologies such as genetic engineering and intertube software are pushing the boundaries of what types of inventions can be protected by utility patents.

Only provisional patent. In the United States, inventors can file a less formal document that proves they had possession of the invention and had sufficiently figured out how to make it work. Once this is done, the invention becomes patent pending. However, if the inventor does not file a formal utility patent within a year of having to file the provisional patent, he or she will forfeit this filing date. Any public disclosures made in reliance on that temporary patent application will now be considered public disclosures to the US Intellectual Property and Trademark Office (USPTO).

the patent protects an ornate design on a functional item. A design patent can protect the shape of a bottle or the design of a shoe, for example. The document is almost entirely made up of images or drawings of the useful item's design. Design patents are notoriously difficult to search because they contain very few words. Design patents have recently been used by software companies to protect elements of interfaces and even the shape of touchscreen devices. A plant patent is exactly what it sounds like it protects new types of plants created through clippings or other nonsexual means. Plant patents, in general, don't cover GM organisms and instead concentrate on traditional horticulture.

3.5 provisional patent:

A provisional patent allows inventors an extra year to decide whether or not to file a utility patent. This is only one example of how an inventor can still use various patent tax forms to reduce risk, hedge a bet, or broaden patent protection. Assume you're whisking eggs and realize that if youbend the tines and flatten them slightly, you can make delicious poached eggs in half the time.

4. CONCLUSION

Customers can identify a company as the supplier of a product or service if it has a logo. Trademarks serve as the foundation for a company's image and standing: they foster a trustworthy connection with customers, allowing a company to build a loyal clientele and increase its goodwill. The trademark law addresses the mechanism for trademark registration, trademark protection, and the protection of fraudulent trademarks. The law also discusses the entitlement obtained through trademark registration, modes of handover and assignment of rights, the nature of infringements, penalties for such breaches, and remedies available to the owner in the event of such infraction.

REFERENCES

[1] N. Papageorgiadis, C. Alexiou, and J. G. Nellis, "International licensing revisited: the role of copyright and trademark enforcement strength," *Eur. J. Innov. Manag.*, 2016, doi: 10.1108/EJIM-03-2015-0014.

[2] L. Tammenlehto, "Copyright and Trademark Crimes in the Nordic Countries: Analysis from the Perspective of the Principle of Legality," *Bergen J. Crim. Law Crim. Justice*, 2020, doi: 10.15845/bjclcj.v8i1.3187.

[3] I. G. N. Bayu Satriawan and M. Marwanto, "Protection of Animated Cartoon Character: Copyright or Trademark?," *J. Magister Huk. Udayana (Udayana Master Law Journal)*, 2021, doi: 10.24843/jmhu.2021.v10.i03.p02.

[4] S. Graham and D. Somaya, "Complementary uses of patents, copyrights and trademarks by software firms: Evidence from litigation," *OECD Conf. Proc. Intellect. Prop. Rights, Innov. Econ. Perform. (Directorate Sci. Technol. Ind. Paris*, 2004.

[5] S. R. Bhat, "Innovation and intellectual property rights law—an overview of the Indian law," *IIMB Manag. Rev.*, 2018, doi: 10.1016/j.iimb.2017.12.003.

[6] G. I. Zekos, "The Influence of Patents , Copyright , Trademarks and Competition on GDP , GDP Growth , Trade and FDI," *IUP J. Manag. Res.*, 2014.

[7] P. C. Patel and J. A. Pearce, "The survival consequences of intellectual property for retail ventures," *J. Retail. Consum. Serv.*, 2018, doi: 10.1016/j.jretconser.2018.03.005.

[8] T. Voss, A. S. Paranjpe, T. G. Cook, and N. D. W. Garrison, "A Short Introduction to Intellectual Property Rights," *Tech. Vasc. Interv. Radiol.*, 2017, doi: 10.1053/j.tvir.2017.04.007.

CHAPTER 19

COMPARATIVE ANALYSIS OF PATENT LAWS IN INDIA

Mr. Amar Anshul, Assistant Professor,
Seedling School of Law & Governance, Jaipur National University, Jaipur, India,
Email Id-amar.anshul@jnujaipur.ac.in

ABSTRACT:

Patents are rights created by statute. Intellectual Property Rights (IPRs) have long played important roles in the innovation systems of most advanced economies. India, these are negative rights and stop everyone except the inventor to get the benefits of the invention. This paper explains the effects of the legislative provisions concerning enforcement and litigation under the Indian Patents Act and its compliance withthe TRIPS agreement. This paper attempts to point out several changes that should be brought about in the system or steps to be taken to provide better Patent protection to the inventors.

KEYWORDS:

Development, Infringement, Monopoly, Patent, Research.

1. INTRODUCTION

One must first comprehend the relationship between law and economics to understand why economics must be used to analyze the law. Prof. Amartya Sen contends that a lack of knowledge of economics is neither a strong prerequisite for serving as a legislator nor a clever path to becoming a formidable legal thinker. Through the lens of economic research, the immediate paper aims to comprehend patent law and how it affects both people and businesses. Given that the basic idea of patent law is to grant monopoly-like rights to the successful applicant, it is crucial to understand how these rights are sought, granted, and ultimately utilized. It follows that economics and law have a lot to learn from one another philosophically and in terms of knowledge. More specifically, the economic analysis of patent law focuses on the idea that while intellectual property rights generally have a positive impact on innovation, they also hurt prices and sales of products incorporating innovations that are less than optimal from a social perspective[1].

The majority of the materials and literary sources are secondary because this article continues to be mostly analytical of patent law in India and worldwide. On the provisions dealing with the main fields of law and economics, particularly those dealing with property law, references to laws, books, and commentaries will be made [2]. The use of pressure was the crucial component of the plaintiff's invention, according to the Bombay High Court in *Lallubhai Chakubhai Jariwala v. Chemical &Co*, and as such, there could be no infringement unless the defendants' use of pressure in their method was shown. *Hindustan Metal Industries v. Biswanath Prasad Radhey Shyam*, the Supreme Court of India established the following principles to evaluate patent infringement:

(1) Read the claims first, then the description;
(2) Identify the prior art;
(3) Describe the improvement over the prior art;

(4) List the broad features of the improvement;
(5) Compare the said broad features with the defendant's process or apparatus; and
(6) Determine whether there has been an infringement if the defendant's process or apparatus is identical to or falls within the purview of the plaintiff's process or apparatus.

1.1. Case-specific exercise for encroachment or non-encroachment:

1. Use by the Government
2. The Exclusion of Research
3. Providing Protected Drugs to Health Foundations
4. Using Safeguarded Innovation on Unfamiliar Vessels
6. Arrangement That Is Bolar-Like. Equal Import
7. Dispute Resolution Machinery in India

In India, there are four dispute resolution machinery with the following powers and duties:

1. Indian Patent Office (IPO)
2. IP Appellate Board (IPAB)
3. District courts, High Court, and Supreme Court

1.2.Duration of patent protection

A patent's ideal lifespan is the consequence of an effective trade-off between promoting new ideas and preventing their widespread use;

a. The marginal societal cost of patent protection (MSC): the extra loss resulting from monopoly pricing when the patent's term is lengthened.
b. The marginal social benefit of patent protection (MSB): rise in socially beneficial technologies with longer patent terms.

The analysis presented above, however, has a serious flaw. Each invention would have a different "breakeven point" in terms of time. It will therefore vary depending on the invention. The average patent lasts 20 years in most nations. The patent length appears to have historical roots (derived mainly from the period necessary to train two sets of apprentices) [3]. If the length of patents were determined by the societal costs and incentive advantages of patents, the type of inventions would determine the length of the patent (for example, the length might be shorter when profits that exceed development cost would be generated in just a few years).

Here, the punitive laws of criminal law can be compared to an analogy. For instance, if an accused is found guilty of grave harm, the sentence is seven years. It is now common knowledge that criminal punishment works as a deterrent to similar or unrelated people committing crimes in the future. In other words, the Legislature determined that a seven-year sentence was sufficient to prevent the criminal from committing the same act again [4].

However, not every crime is the same. A brief sentence may be sufficient for some people to prevent them from committing the same crime again, but even seven years as in the case of our earlier example might not be long enough for others. To preserve social and economic efficiency, punishment therefore genuinely cannot have a set duration. A predetermined duration for the return on investment for innovation is also not very effective. Every innovation, like a criminal, has a different human and financial investment. As a result, the twenty-year time frame that the Patent Act and the rest of the world envisions is, at best, a wild guess.

1.3.Software Patents

Let's think about software patenting as an example. The average lifespan of software is seven to ten years. The rapid pace of hardware development is typically to blame for this. For example, the programs that were popular ten years ago cannot be used on today's IBM computers because they are so much more advanced than they were then.

The cost of unnecessary IT spending on out-of-date software applications is now billions of dollars annually for American businesses. According to reports, it is, therefore, necessary to make sure that the money invested in the development of software is recovered as quickly as possible within ten years, removing the need for software to enjoy twenty years of patent protection [5].

1.4.Patents for Pharmaceuticals

Patent insurance is provided for twenty years following Section 53 of the Licenses Act of 1970. Except for pharmaceuticals and drugs, which had a period of security for a relatively long time before 2002, the patent term was now for a significant amount of time. The question that immediately arises is, "Why is this discrepancy for the pharma industry?" According to the preceding graphic, with a low span, it should follow that either the medication's small social expenditure is extraordinarily large, or its minor social advantage is unusually low, depending on the subsequent element.

The price society would pay for an invention is now known as its marginal social cost. Any government's priority has always been protecting public health; as a result, the availability of pharmaceuticals is heavily stressed, which raises the price that society is ready to pay for that drug. This is particularly true for underdeveloped countries where patent protection prevents the creation of the necessary medications regularly[6]. The Agreement on Trade-Related Aspects of Intellectual Property Rights, which established a twenty-year blanket term, has solved this issue.

2. Social Deadweight Loss

The main disadvantage of intellectual property rights is that they encourage the creation and spread of inventions at monopoly prices, which are insufficient for society. When the monopoly price exceeds the production and distribution costs by a significant margin, this situation may be serious. For instance, computer software is often offered for prices that are several times more than what it costs to produce and distribute, which encourages people to steal it [7]. The monopoly price for the innovation is the presumption under patent law, which is generally practiced on a stand-alone basis. This means that the patentee will maximize her rent during the duration of protection. To be more precise, the patentee will cap output below the level necessary to remain competitive, up until its marginal income equals its marginal cost.

Due to the patentee's monopoly, some customers who would be willing to pay more for the product than its marginal cost are prevented from doing so, which results in a social deadweight loss. In a competitive market, these customers would be able to benefit from trade, but due to the patentee's monopoly, they cannot [8]. To put it another way, deadweight loss happens when a monopolist reduces the amount of an item it produces to increase profits, refusing to sell to certain customers who would be ready to pay more than the cost of producing the good in question. The economist's measurement of the deadweight loss of monopoly is the difference between consumer valuation and production cost for these sales that were not made [9].

The possibility of leveraging patents through trademarks transforms the analysis. When patents can be extended through the creation of brand loyalty, the patentee will strive to maximize her rents not over the twenty-year patent term, but rather over the combined period of patent and trademark protection. Hence, a forward-looking patentee will consider not only current output but also the effects of current output on future demand. In particular, a patentee whose goal is to maximize profits would lower prices throughout the patent period if doing so improves its brand and generates greater revenues in the long run. Thus, it is argued, even patentees who possess monopoly power due to the legal exclusivity granted to them may decide against collecting the entire amount of monopolistic rent made possible by the patent grant. The combination of trademark and patent protection results in two complementary benefits for the owner of intellectual property. First, throughout the patient's life, the restricted exclusivity provided by patent protection could make it easier to build brand loyalty.

Therefore, patent protection raises the brand value of the firm. Second, a patentee's ability to maintain a portion of their market share after the patent protection expires is due to brand loyalty. Accordingly, trademark protection may be added to patent protection. Overall, better protection is provided by combining patents and trademarks than by each one used separately. Unexpectedly, it has been shown that leveraged patents improve welfare since they reduce patentees' propensity to set monopolistic prices, even if they provide higher protection for patentees.

The analysis is fundamentally changed when trademark protection is introduced and lasts longer than the patent term. Trademark protection makes it rational for businesses to invest in the quality of their products by enabling them to build brand loyalty. Trademark protection also puts pressure on businesses to increase sales during the patent term to grow their base of devoted customers for the post-patent period [10]. Because of this, trademark protection may lessen the societal deadweight loss caused by patent protection. That still leaves the fact that patent protection is typically used as a sort of monopoly, which results in higher, unnatural pricing and is therefore a significant drawback for the patent system, unaddressed.

2.1.Patent Race

The uniqueness of an invention is one of the main requirements for an effective patent application. Accordingly, the person who develops the first solution to an issue will be the one to gain from it. The idea of a patent race is introduced here. A legislator trying to create effective patent legislation will run across the issues listed below. Without patent protection, secrecy is the only way to get a return on your investment in research and development [11]. However, it is frequently impossible to protect an invention's significant features. Most product improvements are difficult to keep secret, however, it is very simple to keep the relevant characteristics of process innovations or chemical formulations (Coca-Cola) hidden (competitors will dismantle the product and understand the innovation). As a result, there will be less motivation to spend money on difficult-to-keep-secret product breakthroughs.There won't be as many high-value inventions as may be possible. Two issues might develop from an endless patent monopoly:

1) It would be difficult for ideas to be shared; and underutilization of inventions.
2) It would lead to patent competition between rival innovators (over-investment in research and development.

Let's get into more depth about the second topic. Assume that the current value of the most money that customers of this innovation would be prepared to pay is Rs. 1 Million. This is the social worth of the solution to a specific technological challenge. Assume further that any

business operating in the relevant sector may quickly resolve this issue by allocating Rs. 200,000 to research and development. If the current value of the predicted income is at least Rs. 200,000, a risk-neutral corporation will be ready to invest Rs. 200,000 on research and development. Consider a scenario in which two similar businesses fight for a patent and each estimates a 0.5 chance of being the first inventor and winning the patent. Consequently, each company's anticipated revenue from research and development is equal to 0.5 x 1 million plus 0.5 0 = 500,000 > Rs. 200,000. Both will do research and development as a result.Let's assume for the sake of argument that up to five risk-neutral, identical firms are ready to compete for the patent. The predicted income for each business in this instance equals the R&D expenditures: 0.2 x 1,000,000 plus 0.8 0 equals Rs. 200,000. The result of this scenario is that the invention that could have been done by one company at a research and development cost of Rs. 200,000, is made at a social research and development cost of 5 x 200,000 = 1 Million, the whole potential surplus is transformed into the cost (over-investment).

2.2.Defenses in Suits for Infringement:

Every basis for revoking a patent will be offered as a defense, following Section 107. In a lawsuit alleging infringement, a defendant may assert one or more of the following defenses:

The plaintiff lacks standing to file the lawsuit;

i. The claim of infringement is false;
ii. There was authorization or a license to utilize the innovation;
iii. The alleged infringement of the patent is covered under the scope of innocent infringement or was carried out after the expiration of the patent;
iv. The alleged infringement of the patent is not novel or it is obvious.
v. The principle of estoppels or res judicata is attracted;
vi. The claims alleged to be infringed are invalid;
vii. The existence of a restrictive contract is declared unlawful;
viii. Alleged in ***Cadila Pharmaceuticals Ltd v. Instance Laboratories Pvt Ltd,*** the Gujarat High Court observed that S -107 expressly empowered a defendant to defend any suit for infringement of a patent. Every ground on which a patent could be revoked under S-64 was available as a ground of defense.

2.3.Reliefs That May Be Granted: S- 108

The reliefs available to a successful plaintiff in a suit for infringement include-

(i) An injunction;(ii) Damages; (iii) An account of profits; (iv)an order for deliver-up or destruction (v) Certificate of validity; (vi) Costs.

2.3.1. Injunction:

A civil remedy for prevention is an injunction. There are two types of injunction. Interlocutory/temporary injunctions I and permanent injunctions (ii) both exist. A temporary injunction is only valid for that time frame or until the merits of the case have been fully determined. After the parties have been heard on the merits of the matter, a permanent injunction is issued. The patent's term is the only limitation on the permanent injunction [12].

Principles for the Grant of Temporary Injunction:

The following guidelines are drawn from the ruling in National Research and Development Corporation of Delhi Cloth & General Mills Co Ltd for the granting of a temporary injunction:

The following conditions must be met:

(I) The plaintiff has established a prima facie case;
(II) The patent is valid and infringed;
(III) The patent is old enough and has been used;
(IV) The balance of convenience favors refusing to grant an injunction; and
(V) The plaintiff will suffer irreparable harm if an injunction is denied.

While denying the remedy of a temporary injunction in **Cadila Pharmaceuticals Ltd v. Instacare Laboratories Pvt Ltd**, the Gujarat High Court expressed its opinion that the patent certificate was not a presumptive indication of the patent's validity [13].

In **Franz Xaver Huemer v. New Yash Engineers**, the Delhi High Court also rejected a temporary injunction because the patent had not been used. For several mechanical devices utilized in the textile business, an Australian citizen obtained a patent in this matter in India. In India, the patent was not applied. The plaintiff claimed that the defendant was utilizing his innovation and violating his patent and requested a temporary injunction against it [14] .

2.3.2.*Damages or Account of Profits:*

The plaintiff is entitled to either monetary compensation for losses or a profit account. The choice to select one of them is given to the plaintiff.

2.3.3.Seizure or Forfeiture of Infringing Goods and Implements:

In addition to any other remedies that a court may grant, it may also order the seizure, forfeiture, or destruction, without payment of damages, of any items that are determined to be infringing as well as the materials and tools that are most frequently used in their production.

Right of exclusive licensee to take proceedings against infringement:

When a patent is violated after the license was granted, the exclusive licensee has the right to file a lawsuit under Section 109.

Right of a licensee (under compulsory license) to take proceedings against infringement:

Any individual to whom a compulsory license has been issued according to Section 84 has the right to request that the patentee initiate legal action to stop any infringement of the patent.

2.3.4.Certificate of Validity of Specification:

The Appellate Board or the high court may certify that the validity of that claim was contested in those proceedings and was upheld if any proceedings before the appellate board or a High Court for the revocation of a patent under Section 64 or Section 104 involve the validity of a claim of a specification and that claim is found by the appellate Board or the high court to be valid.

2.3.5. Costs of Suits for Infringement After Obtaining the Certificate:

Insofar as they pertain to the case in which the declaration was conceded, the person will be eligible to request payment of all expenses, charges, and costs associated with any such suit

or proceeding that is properly brought about, unless the court disagrees with the suit's or proceeding's course of action.

3. Role of Indian Judiciary In Protecting Inventors:

There have been significant worries about how the domestic Indian generic industry will fit into the new system of product patents ever since the new law took effect on January 1, 2005. The legal process for infringement cases will resemble that of a typical civil lawsuit, with the High Courts and Supreme Court having appellate jurisdiction.

3.1. Judicial Trends:

The Supreme Court rendered a decision on the issue involving the patent for the use of twin-spark-plug engine technology in **Bajaj Auto Limited v. TVS Motor Company Limited**. The Supreme Court of India has ordered all Indian courts to expedite the trial and resolution of disputes involving intellectual property as a result of this momentous decision ok [15].

Union of India v. Bayer Corporation [16]the Hon'ble High Court of Delhi ruled that as the two Acts have different goals and the Controller of Patents has sole responsibility over setting patent standards, there is no drug-patent linkage system in India. It further ruled that a drug's clearance for the market does not constitute patent infringement. Therefore, it is necessary to show patent infringement in a court of law; it cannot simply be assumed. Drug Authorities do not have the authority to make such decisions.

A patent for a drug that was neither "inventive" nor had a higher "efficacy" was rejected in ***Novartis v. Union of India***. After a 7-year fight, the Supreme Court denied their motion for the grounds listed below First off, no new drugs were invented, as the discovery of an already-existing medicine does not qualify as innovation. In addition to proving the traditional tests of novelty, inventive step, and application, the Supreme Court upheld the idea that under the Indian Patent Act, for the grant of pharmaceutical patents, there is a new test of enhanced therapeutic efficacy for claims that cover incremental changes to existing drugs; Novartis's drug did not meet this requirement. *The fact that the court saw past the technicalities and into the endeavor by these firms to "evergreen" their patents and make them unavailable for low prices led to this decision being a historic one.*

4. CONCLUSION

Although a reasonably well-developed patent system had arisen as early as the 1400s in Venice and had expanded throughout most of Europe and the New World by the end of the 18th century, the system faced serious challenges in the next century, particularly between the years 1850 and 1875. Because monopolistic power damages customers by forcing them to pay high prices and because it can prevent improvements and subsequent developments if patent holders forbid them, criticism of the patent system mirrored disdain for monopoly power. The patent system was disliked by many economists, and in certain nations, like Germany, the economics profession was essentially unified in its opposition.

Simply winning the legal battle won't accomplish the goal. The firm must benefit in some way from that victory. Otherwise, fighting for one's rights is almost pointless. That might not be a wise business decision. In such a situation, it is preferable to let the market determine which product is superior since, as intellectual property rights are increasingly protected, patent holders will undoubtedly want to contest infringement.

The worrying aspect is that procedural matters are becoming more significant than substantive matters. It is past time to streamline the process for patent litigation.

Many European nations planned to amend or abolish patents as a result of the criticism of patents and the potential usefulness of incentives as a replacement, and some did so. Nevertheless, Europe eventually accepted the patent regime, though arguably more for political reasons than to demonstrate a real policy preference for that system.

REFERENCES

[1] P. Brahmi and V. Chaudhary, "Protection of plant varieties: Systems across countries," *Plant Genet. Resour. Characterisation Util.*, 2011, doi: 10.1017/S1479262111000037.

[2] Y. Pai and N. Daryanani, "Patents and competition law in India: CCI's reductionist approach in evaluating competitive harm," *J. Antitrust Enforc.*, 2017, doi: 10.1093/jaenfo/jnx004.

[3] A. Mukherjee, "Patent protection under endogenous product differentiation," *Asia-Pacific J. Account. Econ.*, 2014, doi: 10.1080/16081625.2014.858389.

[4] A. Arora and M. Ceccagnoli, "Patent protection, complementary assets, and firms' incentives for technology licensing," *Manage. Sci.*, 2006, doi: 10.1287/mnsc.1050.0437.

[5] S. E. Abraham, "Software patents in the United States: A balanced approach," *Comput. Law Secur. Rev.*, 2009, doi: 10.1016/j.clsr.2009.09.007.

[6] S. Chaudhuri, P. K. Goldberg, and P. Jia, "Estimating the effects of global patent protection in pharmaceuticals: A case study of quinolones in India," *Am. Econ. Rev.*, 2006, doi: 10.1257/aer.96.5.1477.

[7] F. Savira and Y. Suharsono, "The deadweight loss of social recognition," *J. Chem. Inf. Model.*, 2013.

[8] M. C. Mungan, "Economics of the Independent Invention Defense under Incomplete Information," *Supreme Court Econ. Rev.*, 2012, doi: 10.1086/668519.

[9] J. F. Duffy, "A Minimum Optimal Patent Term," *SSRN Electron. J.*, 2005, doi: 10.2139/ssrn.354282.

[10] R. D. Blair and W. Wang, "Monopoly power and intellectual property," in *The Cambridge Handbook of Antitrust, Intellectual Property, and High Tech*, 2017. doi: 10.1017/9781316671313.012.

[11] H. Al-Fazari and J. Teng, "A model of duopolistic patent contest with private provisions of industry collective goods," *J. Glob. Bus. Adv.*, 2020, doi: 10.1504/JGBA.2020.109146.

[12] A. Mossoff and E. R. Claeys, "Patent injunctions, economics, and rights," *J. Legal Stud.*, 2021, doi: 10.1086/705135.

[13] R. Doshit, *Cadila Pharmaceuticals Ltd v. Instacare Laboratories Pvt Ltd*. 2001.

[14] C M. Rao, *Franz Xaver Huemer v. New Yash Engineers*, vol. AIR 1997 D. 1996.

[15] K.K.SASIDHARAN, *Bajaj Auto Limited v. TVS Motor Company Limited*. 2010.

[16] S. RAVINDRA BHAT, *Bayer Corporation vs Union Of India & Ors*. 2019.

CHAPTER 20

AWARENESS OF CYBER SECURITY PLAYS AN IMPORTANT ROLE IN SOCIETY

Manali Rathore, Assistant Professor,
Seedling School of Law & Governance, Jaipur National University, Jaipur, India,

ABSTRACT:

The protection of computer systems and networks from information disclosure, theft, or damage to their hardware, software, or electronic data, as well as from the interruption or misdirection of the services they provide, is known as computer security, cybersecurity, or information technology security. Cybersecurity is the defense against cyberthreats for systems linked to the internet, including their hardware, software, and data. This article explains the practice utilized by both people and businesses to prevent illegal access to data centers and other computerized systems, as well as the need for cybersecurity knowledge. With the transition of the global corporate environment to cloud data storage and online administration, the need for cybersecurity is at an all-time high. Commercial organization data and user personal data are at risk of being abused as a result of greater internet exposure. New methods to centralize data and automate processes will be crucial for the development of security technologies in the future.

KEYWORDS:

Awareness, Crime, Cybersecurity, Information, Society.

1. INTRODUCTION

Cybersecurity refers to preventing unauthorized or unmanaged access, destruction, or alteration of data, networks, programs, and other information. Because of many security concerns and cyberattacks, cybersecurity is crucial in today's environment. Many businesses create software for data security. The data is shielded by this program. Cybersecurity is crucial since it protects not only our systems from virus attacks but also helps to safeguard information. Cybercrime is when a person or a group of people uses technology, such as a computer, the internet, a smartphone, or other gadgets, to commit a crime. Cybercriminals utilize a wide variety of programs and codes in cyberspace. Through the deployment of malware, they take advantage of flaws in the software and hardware architecture [1]. Identity theft is very widespread, and hacking is a frequent method of breaching computer systems' security and interfering with their operation.

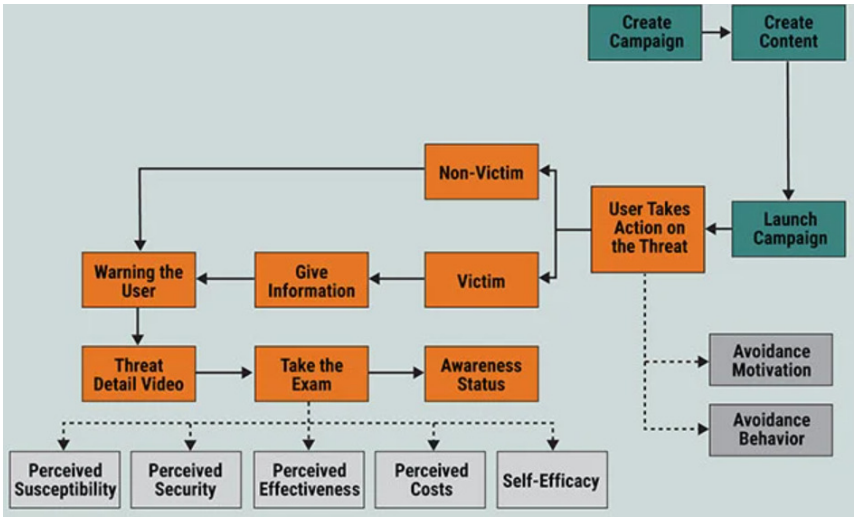

Figure 1: Illustrate the different stages for understanding the prototype of cybersecurity [2]**.**

The best rating was given to the combination of training via online learning and threat simulation. This outcome is used to construct the prototype for measuring and improving cybersecurity awareness. Furthermore, the prototype is used for the acceptance test. The prototype was improved based on the results of the acceptance test, and Figure 1 depicts the finished product. Figure 1 depicts how the simulated cyberthreat is created and communicated to workers without first notifying them since doing so would alert them to the threat. The decision to read the simulated email is the next action, and, following TTAT, this decision may be used to gauge an employee's avoidance motive and behavior [3].

There is a warning message to let workers know they are victims of the assault and must complete an online learning course if they choose to open the email and enter their information. The online learning course imparts information on the many categories of cyberthreats, their effects, and how to defend against them. Employees are expected to complete an online test after completing the online learning course to assess their perceived susceptibility, perceived severity, perceived effectiveness, perceived costs, and perceived self-efficacy [4]. The procedure for understanding cybersecurity awareness is shown in Figure 2 if the workers pass both the simulation and test, indicating that they have a sufficient degree of cybersecurity awareness.

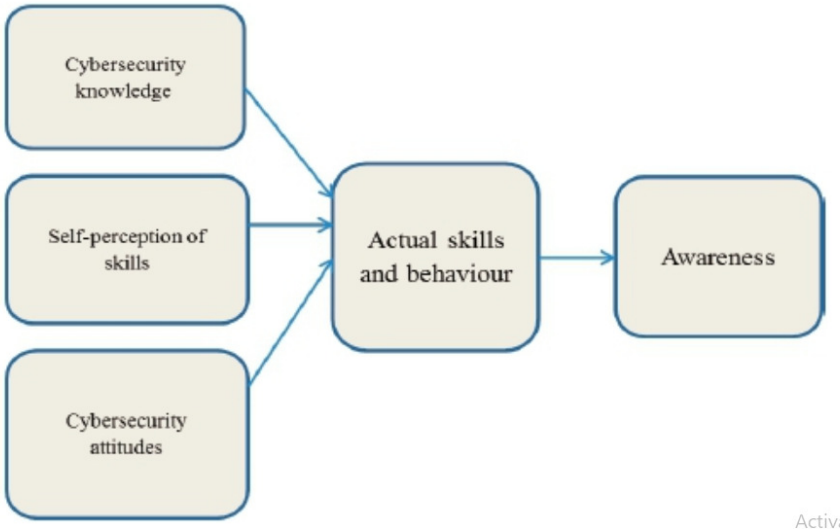

Figure 2: Illustrate the steps for understanding cybersecurity and provide awareness.

Cybercrimes may happen directly, i.e., through propagating computer viruses they attack computers directly. DoS attack is one of the other types. It is an effort to prevent the intended users from using a system or network resource. A host that is linked to the internet has its services temporarily or permanently suspended. Software known as malware is used to obstruct computer operations, collect private computer systems, or obtain sensitive data. Code, scripts, live content, and other types of software are often used to represent it [5]. The term "malware" describes several hostile or invasive software programs, such as Trojan Horses, rootkits, worms, adware, etc.

Independent of a computer network or device, there is another method to conduct cybercrime. It also covers financial scams. It is done to undermine the stability of a nation's financial system, target banking security, steal money via fraud, obtain credit card or debit card information, etc. altering or deleting data to interfere with a website's or service's ability to function. Other examples include spreading pornography, sending threatening emails, creating a false identity, and impersonating another person online. Nowadays, there is a lot of abuse of social media for inciting riots, inciting communal violence, and spreading intolerance [6].

Businesses now understand the need for cybersecurity awareness in reducing possible risks, even if it cannot completely eradicate cybercrime. In actuality, the majority of businesses provide their staff members with some kind of security awareness training. There is potential for improvement in cyber awareness, according to statistics on recent successful data breaches [7]. In the digital era, cybersecurity knowledge is essential. Nevertheless, creating cyber awareness programs may be difficult and time-consuming. Cybercriminals often develop new attack techniques. It's more difficult than it seems to keep up with emerging trends and update training materials.

Since the information and skills that were effective today could not be enough to counteract attacks in the future, this also causes cybersecurity training materials to quickly become out of date. Except in cases when your business employs a fully managed cyber awareness program, developing cybersecurity awareness programs is often a laborious procedure. It may thus be time-consuming and difficult to choose security content, develop resources, and evaluate training materials and tools. Getting staff interested and involved is never easy. Employee involvement may be hampered by repetitive curricula, an abundance of material, the length of the course, and its complexity [8].

Because we are so dependent on information and communication technology (ICT) for every facet of our cyberphysical society, the need for cybersecurity is becoming more and more crucial. Cybersecurity is crucial for people, for both public and private enterprises, yet ensuring security is often challenging. Many governments' websites have weak security and are vulnerable to hacking [9]. Political parties, energy infrastructure providers, water boards, road management, ministries, administrative organizations, NGOs, and even sporting organizations (like the International Olympic Committee), all of which have already been the target of breaches and the theft of information, are also affected by the security issue.

The Stuxnet virus was designed to disrupt a nuclear infrastructure, while the World Anti-Doping Agency (WAPA) attack exposed Olympic athletes' medical records to corrupt them. Thus, it can be claimed that all social actors in our society are impacted by cybersecurity breaches. While a concern for prevention and expenditures in improving cybersecurity have lagged, interest in cybersecurity concerns often focused on events and how to handle them after the fact [10][11]. This is unexpected in a world where hackers and other social actors

are always at war to keep the system secure. Cybersecurity is seen as the next platform in contemporary warfare and is referred to as the new form of war.

People often pick and choose the information they want to receive from a communication. One explanation is that like all individuals, decision- and policy-makers will respond differently to objectively equal presentations of the same issue [12]. It may be challenging to describe cybersecurity problems and the pressing need for legislation in a way that is both obvious and persuasive. All too often, individuals use the danger of cybercrime as a way to fictionalize real-world security issues and incite panic by imagining how they can affect the polity in the future [13]. Furthermore, the distinction between being within or outside a cybersecurity zone is blurred and lost in the way that people and technology interact. Specialists and professionals in cybersecurity have traditionally handled this field since they lack the communication skills necessary to do so. As a result, there is a need for message framing, a technique for explaining a complicated social issue in a manner that makes the major points crystal apparent and insurmountable. Although it is clear that message framing is used and that cybersecurity has to be framed, a thorough study is not yet accessible.

2. DISCUSSION

The percentage of cyber risks and cybercrimes is rising as a result of the tremendous technological advancement and digital transitions taking place throughout the globe. The absolute reliance on the Internet that distance learning, e-government, e-commerce, and many other activities have reached due to the current scenario makes it possible to concentrate on raising cybersecurity awareness. The practice of preventing harm, infection, or illegal access to data, fundamental software, processes, and technologies, as well as to people, devices, and processes is known as cybersecurity [14]. Additionally, the National Cyber Security Authority has released various fundamental controls for cyber security, including asset management, management of login identities and capabilities, mobile device security, email protection, and others. One of these controls is increasing cyber security.

Cybersecurity is crucial since it guards against theft and destruction of many types of data. This covers delicate information, personally identifiable information (PII), protected health information (PHI), personal data, data about intellectual property, and information systems used by the government and businesses. Your company cannot protect itself against data breach operations without a cybersecurity program, making it an unavoidable target for hackers [15]. Due to increased worldwide connection and the use of cloud services like Amazon Web Services to hold private and sensitive data, both inherent risk and residual risk are rising. The probability that your firm may experience a successful cyber attack or data breach is rising as a result of the widespread bad setup of cloud services and more savvy cybercriminals. Business executives cannot exclusively depend on standard cybersecurity tools like firewalls and antivirus software because hackers are growing more cunning and their strategies are becoming more resistant to traditional cyber defenses [16]. To keep safe, it's critical to study every aspect of cybersecurity.

Cyber risks might originate at any level inside your company. To inform personnel about typical cyberthreats including social engineering schemes, phishing, ransomware attacks like WannaCry, and other malware aimed to steal intellectual property or personal data, workplaces must provide cybersecurity awareness training. The practice of defending against and recovering from cyberattacks on computer systems, networks, devices, and software is known as cybersecurity [17]. Your sensitive data is at risk from cyberattacks that are becoming more complex and dynamic as hackers use innovative techniques that combine social engineering and artificial intelligence (AI) to get beyond established data security

measures. The world is becoming more and more dependent on technology, and this dependence will only increase as we develop new technologies that will link to our connected gadgets through Bluetooth and Wi-Fi in the future [18].

Intelligent cloud security solutions should be used in conjunction with strict password regulations like multi-factor authentication to reduce illegal access to safeguard consumer data while embracing new technologies [19]. The significance of cybersecurity is growing. Fundamentally speaking, there is no indication that our civilization will become less dependent on technology. Identity theft-related data dumps are now openly announced on social media sites. Social security numbers, credit card numbers, and bank account information are increasingly kept in cloud storage services like Dropbox and Google Drive.

The truth is that everyone uses computer systems daily, whether they are individuals, small businesses, or giant multinationals. People now have a wide range of possible security risks that weren't there a few decades ago when we combine this with the growth in cloud services, lax cloud service security, smartphones, and the Internet of Things (IoT). Although the two fields' skill sets are growing increasingly comparable, we still need to recognize the distinction between cybersecurity and information security [20].

2.1.The difference between cybersecurity awareness and cybersecurity vigilance:

The human error that allows access to a company's systems and data is a key component of cyberattacks, and sensible cybersecurity awareness training emphasizes this point. We are instructed to choose complex passwords, update them regularly without ever sharing them, never click on a phishing link, and adhere to several other best practices during phishing training. In an ideal world, we would abide by these guidelines. These excellent practices are often forgotten in the imperfect reality where the majority of us live. Businesses that provide training often have yearly sessions, giving staff members plenty of time to forget all they learned. Additionally, over a year, hackers will improve their techniques to the point that previous training is no longer relevant [21].

The majority of training courses cover the dos and don'ts of cybersecurity and increase user awareness of the problems, but they do not promise that workers will apply what they have learned in their daily work activities months from now. That calls for alertness. The distinction between the two is that while vigilance involves anticipating a cyberattack and responding appropriately when one occurs, awareness merely acknowledges its possibility [22]. Employee education and training in cybersecurity awareness is a continuous process that teaches employees about the dangers that lurk in cyberspace, how to stop them, and what to do in the event of a security incident. Additionally, it fosters in them a feeling of proactive accountability for safeguarding the company's assets. Simply put, cybersecurity awareness is being aware of security threats and taking appropriate precautions to reduce risks.

Understanding cybersecurity involves being aware of the most recent security threats, cybersecurity best practices, the risks associated with using the internet, sharing sensitive information online, and other activities. Programs for raising security awareness increase your organization's security posture and tighten its procedures, laying the groundwork for creating a more resilient company. For it to be most useful and successful, cybersecurity awareness must be a company-wide endeavor. Although many firms have top-notch protection systems and precautions in place, security breaches sometimes happen. Sadly, a lot of data breaches have been caused by human mistakes, which has been a key contributing element [23]. Threat actors try to take advantage of this flaw to access a company's systems and networks.

2.2. Need for Cybersecurity Awareness Training:

IT administrators and other employees are now included in cybersecurity awareness training, which had previously been primarily offered to security professionals. The extent of cybersecurity awareness programs may change depending on the workforce, their level of awareness, the budget, and other factors. No matter the scope, the following courses should be part of every program for cybersecurity awareness training.

2.2.1. Email security: One of the most crucial communication tools for organizations nowadays is email. It is, however, also the starting place for several cybercrimes, such as phishing, ransomware, malware, and BEC. Email is the primary method used by 94% of all harmful ransomware and other malware to infiltrate a business. To safeguard your staff and company from nefarious email assaults, email security training is essential. Employees will benefit from email security training by learning to avoid dangerous links and attachments**.**

2.2.2. Phishing and social engineering: The key entry point for threat actors is the human assault surface. Attackers who use social engineering are knowledgeable of how others think and behave. They use this information to manipulate targets' behavior and emotions to persuade them to do what they want. For instance, exchanging credentials, allowing system access, releasing private information, transferring money, and so on. According to Verizon's 2021 Data Breach Investigations Report, phishing was engaged in more than 35% of data breaches. Phishing and social engineering assaults are very effective because they are targeted and persuasive. However, with the appropriate instruction and expertise, your staff can recognize red flags and significantly lower the likelihood of falling for these con games.

2.2.3. Ransomware and malware: Phishing emails are used to introduce malware, such as ransomware, into a business. An estimated 300,000 new malware samples are produced every day. According to SonicWall's 2021 Cyber Threat Report, ransomware incidents rose by a staggering 48% in 2020. Employees who get ransomware awareness training will better grasp how these assaults are carried out, the strategies threat actors deploy, and the steps they may take to combat the growing number of ransomware attacks.

2.2.4. Browser security: Since web browsers are the primary access points to the internet and store a significant amount of sensitive data, including personal data, they are prime targets for hackers. You can't always trust the websites you visit online. To protect the privacy and access the internet securely, browser/internet security training that covers best practices, browser security advice, the many sorts of browser risks, and internet and social media regulations may be very helpful.

2.2.5. Information security: The most valuable asset in a company is its information. Because of this, everyone should be responsible for ensuring its availability, confidentiality, and integrity. The importance of data security and your obligations to secure the data must be emphasized in the training programs you provide. Your staff should get training on safe handling, sharing, storing, and disposal of sensitive information. Understanding exactly what a breach entails in terms of legal and regulatory duties is essential. Employees should also get incident reporting training to address problems swiftly and reduce risk**.**

2.2.6. *Remote work protocol:* Working remotely has become commonplace, as shown by the fact that most firms worldwide have adopted a hybrid work paradigm. Organizations now have to assure safety and security not just at the workplace but also at home or elsewhere, which presents increased obstacles. Additionally, this increases security threats. However, with the proper training and equipment for your staff, these hazards may be considerably decreased. The risks of connecting to unsecured public Wi-Fi networks, the use of personal devices and unauthorized software, and the significance of VPNs for additional layers of security, to name a few, must be covered in your training programs.

2.2.7. *Physical security:* Physical security covers a wide range of activities, from being cautious of shoulder surfers to safeguarding the computers and mobile devices given by your employer from possible security hazards. For instance, securing the gadgets while leaving the room, maintaining a tidy workspace, preventing tailgating, and keeping private documents and printed materials in a safe location**.**

2.2.8. *Removable media security:* Data may be copied, transferred, and stored easily using removable media, such as USB drives, CDs, portable hard drives, cellphones, SD cards, and more. Risks include data exposure, malware or virus infection, data loss, and data theft. Teach your staff about the organization's policy on portable media, the dangers of using them, particularly unauthorized or untrusted ones, the significance of the policy, and the consequences of not adhering to it.

2.2.9. *Password security:* Consumers reported cybercrime to the Federal Trade Commission (FTC) over 5.7 million times in 2021, with identity theft accounting for 25% of all complaints. In an environment that is rife with threats nowadays, the need of having a strong password is crucial. Password management and best practices, such as what makes a secure password and how to create one, must be included in security awareness training. To avoid account breaches, your staff members must also utilize multifactor authentication (MFA) wherever feasible.

2.2.10. *Incident response:* It is not sufficient to have an incident response (IR) team and plan. Additionally, you need to inform your staff of their obligations in the case of a security problem. Unavoidable security events are the unpleasant truth. Your company's ability to handle such occurrences might be the difference between dealing with legal and regulatory difficulties, swiftly resolving crises, and preventing more harm.

2.3.*Cyber security domains:*

Layers of defense are included in a solid cybersecurity plan to combat cybercrime, such as attempts to access, modify, or delete data; demand money from users or the company; or obstruct regular business activities. Countermeasures need to focus on:

2.3.1. *Critical infrastructure security:* Procedures for safeguarding the networks, computers, and other assets that society depends on for economic viability, public safety, and/or national security. To assist enterprises in this area, the National Institute of Standards and Technology (NIST) has developed a cybersecurity framework, and the U.S. Department of Homeland Security (DHS) offers further advice.

2.3.2. *Network security:* A computer network's security measures, including wired and wireless (Wi-Fi) connections, are designed to deter hackers.

2.3.3. *Application security:* Processes that aid in protecting cloud-based and on-premises apps. Applications should be designed with security in mind from the beginning, taking into account user authentication, data handling, etc.

2.3.4. *Cloud security:* Specifically, genuine confidential computing that secures consumer privacy, business needs, and regulatory compliance standards by encrypting cloud data while it is at rest (in storage), in motion (as it moves to, from, and within the cloud), and in use (during processing).

2.3.5. *Information security:* Your most sensitive data is protected by data-protection procedures like the General Data Protection Regulation, or GDPR, which prevent unauthorized access, disclosure, or theft.

2.3.6. *End-user education:* Increasing security awareness within the company to improve endpoint security. Users may be taught, for instance, to discard dubious email attachments and steer clear of unidentified USB devices.

2.3.7. *Disaster recovery/business continuity planning:* Tools and processes for reacting to unforeseen occurrences, such as power outages, cybersecurity attacks, or natural catastrophes, with the least possible impact on critical activities.

2.3.8. *Storage security:* delivers incredibly strong data resilience with many security measures. This includes immutable and isolated data copies as well as encryption. These continue to be in the same pool so that they can be easily restored to aid in recovery, reducing the effects of a cyberattack.

2.3.9. *Mobile security:* With app security, container app security, and secure mobile mail, you can control and protect your mobile workforce.

Cybersecurity awareness training teaches your staff how to recognize possible risks, how to prevent being a victim of these sneaky attacks, how hackers utilize malevolent techniques, and how they might be easy targets. It equips your personnel with the necessary information and tools to recognize and report any hazards before they do any harm. Neglecting or failing to undertake cybersecurity awareness training regularly may have major negative effects on your firm, including fines, financial loss and remediation costs, loss of intellectual property, a tarnished corporate image, a loss of client confidence, and others. Since your people are your weakest link, your company's cybersecurity plan can only be as effective as they are.

Many businesses provide training courses to help employees become more knowledgeable about cybersecurity. However, corporations may not get enough training to be able to handle cyberthreats and assaults. They cannot develop cybersecurity awareness and an incident response strategy since the majority of cybersecurity awareness training concentrates on theory. This means that, in addition to a training program, staff members and management must participate in cyberdrills virtual fire drills that simulate real-world cyberincidents. An exercise known as a "cyberdrill" mimics a cyberattack on workers or individuals whose jobs include responding to cyberincidents. These exercises help them get more used to the dangers. Cyberdrills may also detect if a worker has a high chance of falling prey to online attacks. The organization achieves a level of cyberresilience that is particularly strong against the effects of assaults by responding quickly to an occurrence. The organization's ability to uphold the service level agreement (SLA) with consumers may be aided by this reaction. Therefore, the cyberdrills may aid in increasing employee awareness of cyberthreats and helping them respond to them more effectively.

3. CONCLUSION

The current study focuses on cyber security awareness campaigns and seeks to uncover crucial security aspects that may prevent them from successfully altering people's behavior. The anticipated results have not been achieved despite past and present attempts to enhance information security procedures and advance a sustainable society. Therefore, it is crucial to critically consider the difficulties associated with enhancing information security practices among customers, workers, and citizens. Our study specifically takes into account these issues from a psychological standpoint since we think that knowing how people perceive dangers is essential to developing persuasive awareness campaigns. Information regarding threats and defensive behaviors is not enough to change behavior. People must be able to comprehend and implement the advice, as well as be motivated and eager to do so, all of which need changes in attitudes and intents.

REFERENCES

[1] M. H. M. Bin Ibrahim, "The Awareness of Cyber Security in Distance Learning," *Sci. J. King Faisal Univ. Basic Appl. Sci.*, 2021, doi: 10.37575/h/edu/0089.

[2] Rishikesh Rao, "Increasing Awareness for Cyber Security in the Corporate Sector," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, 2021, doi: 10.32628/cseit217653.

[3] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*. 2020. doi: 10.1016/j.dcan.2019.01.005.

[4] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," *Heliyon*, 2021, doi: 10.1016/j.heliyon.2021.e06016.

[5] B. Svilicic, D. Brčić, S. Žuškin, and D. Kalebić, "Raising awareness on cyber security of ecdis," *TransNav*, 2019, doi: 10.12716/1001.13.01.24.

[6] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," in *Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018*, 2019. doi: 10.1109/TALE.2018.8615162.

[7] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2018.09.063.

[8] P. T. Mai and A. Tick, "Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in hungary and Vietnam," *Acta Polytech. Hungarica*, 2021, doi: 10.12700/APH.18.8.2021.8.4.

[9] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors Related to Cyber Security Behavior," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3007867.

[10] I. Mraković and R. Vojinović, "Evaluation of Montenegrin seafarers' awareness of cyber security," *Trans. Marit. Sci.*, 2020, doi: 10.7225/toms.v09n02.005.

[11] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Reports*, 2021, doi: 10.1016/j.egyr.2021.08.124.

[12] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A Serious Game for Cyber Security Awareness and Education," *Comput. Secur.*, vol. 95, 2020, doi: 10.1016/j.cose.2020.101827.

[13] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A Review of Using Gaming Technology for Cyber-Security Awareness," *Int. J. Inf. Secur. Res.*, 2016, doi: 10.20533/ijisr.2042.4639.2016.0076.

[14] P. Rathod and A. B. Potdar, "Study of awareness of cyber-security among medical students," *Indian J. Forensic Med. Toxicol.*, 2019, doi: 10.5958/0973-9130.2019.00040.9.

[15] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3041951.

[16] Y. Wang, B. Qi, H. X. Zou, and J. X. Li, "Framework of raising cyber security awareness," in *International Conference on Communication Technology Proceedings, ICCT*, 2019. doi: 10.1109/ICCT.2018.8599967.

[17] F. Nejabatkhah, Y. W. Li, H. Liang, and R. R. Ahrabi, "Cyber-security of smart microgrids: A survey," *Energies*. 2021. doi: 10.3390/en14010027.

[18] I. Mraković and R. Vojinović, "Evaluation of Montenegrin Seafarer's Awareness of Cyber Security," *Trans. Marit. Sci.*, 2020, doi: 10.7225/toms.v09.n02.005.

[19] K. Renaud and J. Ophoff, "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs," *Organ. Cybersecurity J. Pract. Process People*, 2021, doi: 10.1108/ocj-03-2021-0004.

[20] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.4.4(12).

[21] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arab. J. Sci. Eng.*, 2020, doi: 10.1007/s13369-019-04319-2.

[22] M. A. Pitchan and S. Z. Omar, "Cyber security policy: Review on netizen awareness and laws," *J. Komun. Malaysian J. Commun.*, 2019, doi: 10.17576/JKMJC-2019-3501-08.

[23] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustain. Cities Soc.*, 2021, doi: 10.1016/j.scs.2020.102655.