Cybercrime: Challenges and Opportunities of Law for National Security and Privacy in the Digital Age

Abstract

The rapid rise of technological developments such as Digital Technologies, Artificial Intelligence and Internet Systems has resulted in significant changes in National Security Strategy and has also intensified Privacy, Data Protection and Civil Liberties concerns. Cybercrime is an important, newly emerging non-traditional Security Threat which exploits the vulnerabilities of Technology and crosses International Boundaries, thereby creating difficulties for current Legal and Institutional frameworks. This research will provide a critical analysis of how the relationship between National Security Imperatives and Privacy of Individuals in the Digital Age is changing, through a Comparative Legal Analysis of India, European Union, United States and United Kingdom. The Cybercrime Study examines both the characteristics and extent of cybercrime, the development of laws protecting privacy, the frameworks used by governments and corporations to obtain information on individual users, and the function of courts as regulators of government activity. This research examines the effect of New Technology (specifically Artificial Intelligence) and Big Data and automized Decision Systems on Cyber Security Systems. It has utilized a combination of doctrinal and comparative methods. The study has found that there are differences between jurisdictions in regards to: (I): enforcement strength, (II): judiciary capacity, (III): liability of the intermediary parties and (IV) co-operation of cross-border jurisdictions. The Results of this research are that while the EU has established a legal framework based on a rights approach and a harmonized

approach which places a strong emphasis on data protection and judicial protection, India and the United States have adopted a security-oriented approach and that both have expanded and continue to expand their surveillance powers and hence face greater enforcement issues. The United Kingdom shows a fairly even blend of aggressive law enforcement with the judicial system providing checks and balances. The research has found that Cyber Legal Frameworks have to evolve so that they can be adapted to changes in technology, there will be more judicial oversight, and international co-operation on cybercrime should improve. The study suggests creating technology-neutral legal systems that consider National Security interests with strong Privacy and Data Protection standards in the Digital Age.

Keywords: *Cybercrime; National Security; Privacy Protection; Data Protection Law; Digital Surveillance; Artificial Intelligence; Comparative Cyber Law; Judicial Oversight; Cyber Governance; Emerging Technologies*

Table of contents

List of Tables

List of Figures

CHAPTER 1

INTRODUCTION

Digital Technologies and Internet Enabled Systems, have rapidly expanded into the areas of governance and communication (social network) and security systems over the last decade. While these digital tools have enabled States to have improved capabilities for crime prevention, gathering intelligence, and managing national security; at the same time, they raise important questions related to the privacy of our information[1]. The greater use of surveillance systems, computerized data handling and AI has heightened the potential legal conflict between a nation's need for security-type measures and the people's right to privacy [2]. With the speed of change in the field of digital technology and the internet, our lifestyle, work and methods of communication have changed rapidly. This change has created a wealth of advantages and potential to create numerous ways to benefit from those advantages. One of the key characteristics of the 21st century is the multitude of digital devices and platforms [3]. The last several years regarding the ways that digital crime, specifically cybercrime, is evolving, how it

behaves in relation to other non-digital types of criminal acts (telephone scams, fraud, etc.), and also what distinguishes them from one another, as a result of the ever-changing nature of digital technology [4]. Recently, the idea of governance has become more prominent and has an impact on management systems worldwide. Therefore, the idea of cyber governance naturally developed as a reflection of this in cyberspace. To achieve success in cyber governance, it is necessary to provide features such as openness, transparency, participation, and accountability in the concept of governance, and human rights must also be protected [5]. As part of the digital revolution, data privacy and the emergence of ethical issues are still being thoroughly examined. Protecting data privacy is a basic right that is frequently disregarded when data is transferred for business and research purposes [6]. Cybercrime is the most recent type of crime that affects a large number of individuals [7]. This is the biggest challenge for lawmakers, prosecutors, and law enforcement. Acts such as altering source code, hacking in Computer systems, distributing pornographic content, and misusing digital signatures or licenses are all covered under the criminal provisions [8].

National security concerns include supply chain management, industry, law enforcement, health, food, and other non-traditional security issues [9]. AI is a fascinating technology that can provide analytics and intelligence to defend against constantly changing cyber-attacks by quickly analyzing millions of events and monitoring a wide range of cyber-threats to foresee and take preventative action. Numerous studies have been conducted to address issues pertaining to the identification, protection, detection, reaction, and recovery from cyber-attacks as a result of the thriving field of cybersecurity and the growing interest of academics from both AI and cybersecurity [10]. A number of nations have implemented legal frameworks designed to strike a balance between privacy protection and security requirements. The General Data Protection Regulation (GDPR) in the EU, the Information Technology Act of 2000 in India, the Computer Fraud and Abuse Act in the US, and the Computer Misuse Act in the UK are a few notable examples [11–14]. The digital age poses challenges in balancing national security and privacy due to borderless cybercrime, rapid technological evolution, and

expansive surveillance powers. The current legal frameworks exhibit a number of serious privacy concerns as a result of utilizing artificial intelligence (AI), Big Data, different jurisdictional legislation conflicting with each other, a lack of speed when adapting laws to new technology, and various enforcement issues arising from inconsistencies between jurisdictions [15]. Due to how the above-mentioned limitations affect the existing legal framework, individuals are not as well protected, and there is a disparity among various countries regarding the effectiveness of the cyber governance laws. Therefore, new flexible legal frameworks need to be created; develop enhanced judicial oversight; and encourage greater international collaboration to meet these challenges. Comparative studies of different countries' laws can help identify effective strategies to balance national security objectives with strong privacy protection.

1.1 Problem Statement

Digital Growth will be a major force in our society for years to come, however, as digital Technologies continue to grow rapidly, many have become concerned about how data is collected, how much data will be collected, and where that data will ultimately go and how that may be used for many different purposes. It will also lead to a further erosion of privacy rights across all levels of society.

- The current law is unable to appropriately balance national security with having protection over individual privacy.
- The borderless nature of cybercrime has created numerous jurisdictions, which create many challenges for investigators, prosecutors and enforcers.
- Cybercrime laws and Data Protection laws are not able to keep up with the rate of growth of new technologies, such as Big Data and Artificial Intelligence.
- Increasing use of Automated Decision Making and Digital Surveillance Systems raises many ethical, accountability and transparency issues.
- There are weak enforcement mechanisms and limited technical expertise for cyber & privacy laws.
- Judicial oversight is lacking for surveillance, which decreases civil liberties and public trust.
- Countries have developed an inconsistent and regulatory gap between their legal methods of protecting privacy while maintaining security.

1.2 Research gap:

Most existing research examines issues of national security and privacy separately and so fail to provide a fully integrated view of both issues.

- There is insufficient comprehensive comparative legal research regarding India, EU, USA and UK under one analytical framework.
- The benefits of judicial control over digital snooping activities has not received much attention in scholarly research
- The effects of cybersecurity-related decisions made by computers and artificial intelligence have not been investigated sufficiently from both legal and ethical perspectives.
- Creating and enforcing laws related to cybercrime is typically described descriptively but does not address the way these factors affect the practical implementation of law.
- At this time, there has not been enough academic research published on establishing an internationally harmonized body of law to deal with cyber threat across borders in an effective manner.
- At present, there has not been enough research done to develop a balanced legal model that will protect and enhance national security at the same time as protecting the fundamental right to privacy of the users of Technology.

1.3 Aim and Objectives:

The primary aim of this research is to critically examine the challenges and opportunities of legal frameworks governing national security and privacy in the digital age, and focusing on evaluating the effectiveness of existing cyber laws through a comparative legal perspective

Objectives

The objectives of the research include the following:

- Investigate and obtain a better understanding of the nature of cybercriminal acts, their magnitude, and consequences; as well as how these acts are being committed on a variety of online platforms affecting the security of Nations.
- To understand the various types of laws relating to Data Privacy and Protection in different Regions/Countries.
- Assess whether or not existing Cyber laws are performing effectively in striking a balance between National Security requirements and individuals' Privacy rights
- The challenges presented through compliance and regulation regarding emerging technologies for enforcement, governance, regulatory modification/implementation, etc.
- Comparative legal analysis of certain legal systems with respect to cyber and privacy laws (India, European Union, United States, United Kingdom).
- Investigate how Judges and how the Constitution protect against surveillance and collecting data for National Security.
- Assess the ethical and accountability problems associated with the National Security, Law Enforcement and Artificial Intelligence and Automated Decision Making.

- Provide recommendations for creating a balanced legal framework to meet the requirements of National Security while affording robust protection of privacy and data.

Research Questions

- What are the key legal challenges in balancing national security and privacy in the digital age?
- To what extent do national security measures impact data protection and civil liberties?
- How do emerging technologies such as artificial intelligence and big data influence cyber law and privacy regulation?
- What comparative principles on harmonizing security and privacy can be learnt from the legal strategies of India, the EU, the USA, and the UK?
- How is accountability and proportionality in national security monitoring measures ensured by judicial oversight?
- What moral and legal issues are raised by the application of automated technologies and artificial intelligence in cybersecurity governance?
- In the digital age, how can legislative frameworks be changed to strike a long-term balance between privacy and national security?

1.4 Thesis Organization

The remaining points of the thesis are as follows:

Chapter 1 – Introduction:

This chapter presents an overview of cybercrime in this digital age and how it is affecting our country's perspectives toward National Security and private lives. The reader will understand the historical context for this research; a definition of the problem it addresses; the aim of research and questions; an explanation of why the research is important; as well as detail on the extent and methods of research carried out by the author. The chapter wraps up with a summary of what we can expect to see throughout our work.

Chapter 2 – Conceptual and Theoretical Framework:

This chapter provides a structured approach to conceptualizing Cyber Crime from the viewpoint of Digital Governance. Furthermore, several overarching perspectives on theoretical approaches to the intersectionality and interactivity of both areas are presented. These include but are not limited to: Cyber Crime Typologies; National Security Frameworks; Privacy Rights; Surveillance Theories; and Cyber Governance Models. All of these provide the analytical framework for the study of this chapter.

Chapter 3 – Review of Literature:

In this chapter a detailed examination of existing national and global literature regarding cyberspace crime, the protection of privacy, Governmental monitoring and safety, and lastly National Security will be conducted. Major contributions made in the scholarly community will be detailed, gaps found in current Research will be discussed, and reasons for conducting the present study will be established.

Chapter 4 – Cybercrime, National Security, and Privacy Challenges:

This chapter looks at the legal and practical issues cybercrime poses for achieving both national security and the preservation of individual right to privacy. Topics include Surveillance/Digital Intelligence, Data Protection, Emerging Technologies, and Enforcement Limitations in the Digital Environment.

Chapter 5 – National Legal Frameworks on Cybercrime:

This Chapter reviews the cyber law framework established by India`s cyber law statutes, focusing primarily on India`s cyber laws, namely, the Information Technology Act of 2000, the Digital Personal Data Protection Act of 2023, and other related laws, and the cybercrimes issue, as well as the state's protection of privacy and the state's interests in protecting national security, against the backdrop of cyber law.

Chapter 6 – Comparative Analysis of Cyber Laws:

The comparison of Cyber Laws between India, the European Union, The United States and The United Kingdom is outlined in this section of the study; the purpose being to demonstrate each country's unique ways to manage the enforcement of Cyber Laws, as well as each country's approach to Civil Liberty Protection. The analysis will show how each country has established methods for enforcement as well as means to achieve Civil Liberty Compliance.

Chapter 7 – Findings, Opportunities, and Conclusion:

This final chapter presents a brief overview of the key results and conclusions from this research, highlights specific barriers and opportunities within the legal landscape, and provides specific legislative recommendations to improve cyber law. Moreover, the chapter also includes some suggestions for future research within the areas associated with cybercrime and digital governance. Fig 1.1 represents Thesis Organization.

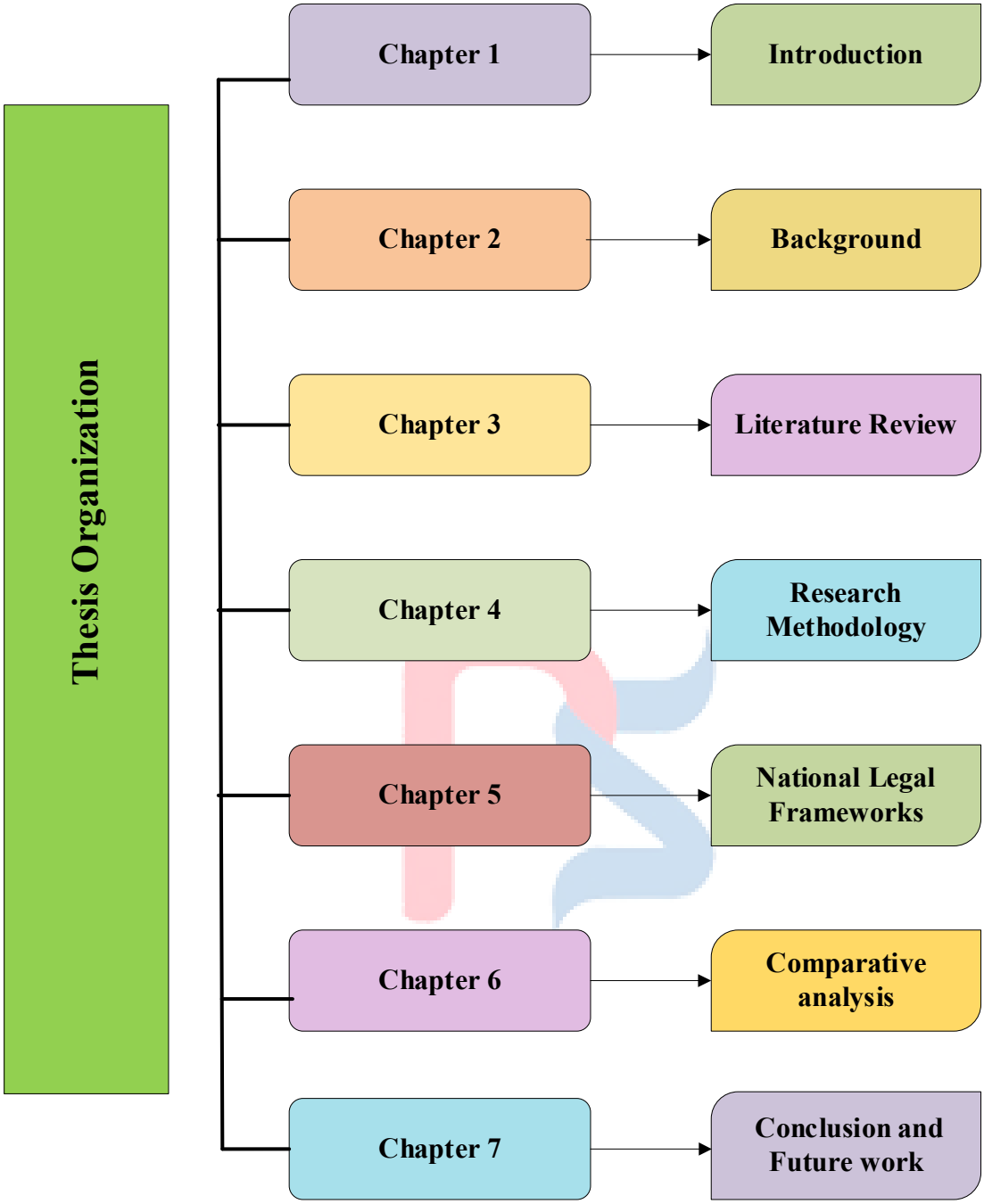

Fig 1. 1 Thesis Organisation

CHAPTER 2

CONCEPTUAL & THEORETICAL FRAMEWORK

The conceptual and theoretical framework of cybercrime and the challenges to its regulation are covered in this chapter. A definition of cybercrime, as well as its characteristics, types, and changes in the past, are included. Other topics addressed include privacy and data protection, cyber surveillance, and cyber governance. The legal theory relating to cybercrime, jurisdictional and technological risks associated with cybercrime, provide a coherent structure to assist in the development of the analytical framework found in the rest of the chapters.

2.1 Concept and Nature of Cybercrime

In the modern world, crime is a social phenomenon. Unfortunately, despite our best efforts, a cybercrime free society will never be possible. What hope do we have for reducing crime in the virtual environment, which is infinitely more unreal, everlasting, and unaccountable in the eyes of the law than the physical world? The type, scope, and significance of crime changes with time.

It is impossible to imagine a society free of crime since crime is inseparably linked up with civilization. Consequently, the structure of a society has an impact on the kind of crime that is committed. As a civilization grows in intricacy, so does the complex nature of the crime which emerges in its immediate surroundings. To understand crime in a culture, it is essential and critical to examine all the factors that influence and contribute to it.

The socio, economic and political structures of society must comprehend crime and the measures that can be taken to reduce it. While determining the nature and scope of a crime, the corrective and preventative actions implemented by the machinery designed to govern crime as well as deviant behaviour in society are being considered. Technological advancement has brought new socio-economic as well as political challenges in society. With the advent of computer technology, it is now possible for anyone, wherever in the world, to have instant virtual access to any type of information. Modern technology has eliminated the constraints of time and place. However, given the great advantages of having computers nowadays, jurisdictional issues have arisen while dealing with such cases. Human behaviour that are restricted by criminal law and in which the State levies penalty under criminal law are to be considered as crimes. Cybercrime refers to criminal acts conducted via computers and networks. Online scam, identity fraud, credit card account frauds, hate crimes, telemarketing, phishing, etc. are all examples of crimes that can be undertaken via the Internet. Identifying the jurisdiction of a multinational transaction through the internet might be tricky.

When courts faced jurisdictional issues, they were unable to decide the proper forum for hearing cases concerning cybercrime since cyberspace or the online environment is borderless in comparison to the external reality, making cybercrime particularly difficult to handle. The problem of cybercrime using local machinery becomes difficult since our machinery is incompatible with dealing with global crimes. Because cybercrime is different from other types of crime, the law in the region is insufficient to regulate it. Cybercrime has become a global phenomenon; nationwide generalization of crime is no longer feasible in the current situation.

Our understanding and regulation of cybercrime cannot be limited to a single country and must be global. Only by enacting new laws and preparing global preventive and defensive mechanisms will we be able to defend our civilization from this scourge known as "Cybercrime." As a result, the prospect of cyber terrorism poses a severe threat to the globe and its institutions. Terrorist organizations use technology to preach hatred and recruit militants, who are then trained utilizing teaching tools. They're also developing websites that teach people how to use firearms and construct bombs, among other things [16].

2.2 Brief history of Cybercrime:

The Brief history of Cybercrime has been divided into four phases of development:

2.2.1 First Phase:

Information systems have impacted a nation's military strategy and foreign attacks since ancient times. The Egyptians employed an encryption and decryption technique about 1900 BC. The origins of hacking can be found in the 1870s. Teenagers typically utilize their new phones for phone phreaking. William Frederick Friedman was recognized as the father of American cryptanalysis and was the primary codebreaker of Japan's Purple Machine during World War II. 1918 book on cryptography continues to serve as a guide for preventing and controlling cybercrimes.

2.2.2 Second phase:

In the 1960s, telephone phreaking of 1870 became hacking. The telephone operators became increasingly curious about computer systems and how to use them in their daily activities. IT professionals with access to new technology, such as developers, engineers, and administrators, were the first to commit cybercrime. The Massachusetts Institute of Technology's (MIT) AI lab was converted into a testing ground for cybercriminals. At the time, the phrase "Hacker" was regarded a significant term, and only computer specialists with a high level of technological understanding were engaged in such operations. By implementing new IT, a Minnesota bank was robbed by cybercriminals in who discovered how to use MIT computers to produce the tones of phone with the goal of using the telephone companies' long-distance services.

2.2.3 Third Phase:

By 1970, users all around the world had access to the internet, and a brand-new cybercrime called cyber pornography had surfaced. Program code was first used by the hackers [17].

2.2.4 Four Phase:

Approximately 6000 out of 60,000 hosts on the Internet were impacted in 1988 by an internet worm, which is a little computer software. The timeline of several cybercrimes from the first one in 1834 to the most recent one in 2021 is shown here to illustrate how technical advancement affects cybercrime. Table 2.1 represents Cybercrime incidents. The Cybercrime Timeline table (1834-2021) is presented as follows:

Table 2. 1Cybercrime Incidents

Year	Place	Types of Cybercrime/incidents
1834	France	Hackers infiltrated the French Telegraph System to steal stock market data (world's first cybercrime).
1878	New York, USA	Misuse of telephone system - young boys disrupted Bell Telephone customer service calls.
1955	USA	Phone phreaking by David Condon using tones to manipulate phone networks.
1957	USA	Joe Engressia (7-year-old) becomes first known "phone phreak"-used 2600 Hz whistle to control phone systems.

1969	University of Washington, USA	RABBITS Virus released-first self-replicating malware overloads system.
1970	USA	Kevin Mitnick uses social engineering to gain unauthorized access to Motorola, Nokia systems.
1973	New York, USA	Bank teller embezzles $2M using a computer system.

1981	USA	Ian Murphy ("Captain Zap") hacks AT&T's system, altering billing clock times.
1982	Siberia (USSR)	CIA plants logic bomb in pipeline system causing explosion.
1984	USA	Robert Morris releases the Morris Worm, first major Internet worm.
1988	USA	Morris Worm strikes again, infecting thousands of systems.
1989	UK	Trojan Horse "AIDS Diskette" sent to researchers, encrypting files.
1994	USA	Hackers (DataStream Cowboy & Kuji) plant password sniffer on US Air Force network.

1995	USA / Russia	Vladimir Levin hacks Citibank, transferring $10M globally.
1999	Global	Melissa Virus spreads via Microsoft Word email attachments.
2000	USA / Russia	Barry Schlossberg (Lou Cipher) extorts $1.4M from CD Universe.
2002	Global	Major Distributed Denial-of-Service (DDoS) attack on the internet.
2004	USA	Nigerian national breaches ChoicePoint database- 35,000 records stolen.
2006	USA	TJX data breach, 45 million card records stolen used for fraudulent shopping.

2008	USA	Heartland Payment Systems breach, 134 million credit cards compromised via SQL injection.
2010	Iran	Stuxnet Worm, first cyberweapon targeting industrial control systems.
2011	USA	Epsilon data breach exposes millions of customer emails.
2013	Global	Russian cyber gang attacks 100+ banks and organizations worldwide.
2015	Global	Locker Pin ransomware locks Android phones; users extorted for $500.
2016	USA	WikiLeaks publishes Democratic National Committee (DNC) emails before elections.

2017	USA	Equifax breach exposes 143 million records including SSNs, DOBs, etc.
2017	Global	WannaCry ransomware attacks 150 countries, demanding $300 per system.
2017	USA/Europe	Chipotle restaurants targeted via phishing, customer card data stolen.
2018	Global	Marriott Hotels breach via Remote Access Trojan; passport & credit card data stolen.
2018	China	Telemarketing employee leaks 1.1 million records including Alibaba customer data.
2019	Global	Facebook data leak, 530 million user records exposed.
2020	China	Sina Weibo breach, 538 million user details leaked to dark web.

2020	USA	FireEye hacked; Red Team penetration-testing tools stolen; SolarWinds supply-chain attack revealed.
2021	USA	Colonial Pipeline ransomware attack system shutdown; $5M ransom paid.
2021	Global	Accenture breached by Lock Bit ransomware group $50M ransom demanded.
2021	Kaseya (VSA software) / many MSPs globally	Ransomware attack by REvil exploited vulnerability in VSA to hit thousands of downstream customers.
2021	Transnet (South Africa port operator)	Ransomware attack disrupted key maritime infrastructure (ports) major operational consequences.

2023	Capita (UK outsourcing / services provider)	Data-breach + ransomware + data exfiltration: ~6.6 million individuals' data stolen.Regulatory consequences & large fines.
2023	British Library (UK)	Ransomware / cyberattack led to leak of ~600 GB of documents; serious disruption catalogue and public services impacted for months.
2023	Kyivstar (Ukraine telecom)	Large-scale cyberattack disrupting mobile/internet services across Ukraine; hit civilian infrastructure including air-raid warning systems.
2024	Snowflake (cloud data-warehousing platform) many enterprise clients	Massive data breach via cloud misconfigurations & vulnerabilities: sensitive and personal data from many major clients exposed.

2024	Lock Bit (ransomware-as-a-service group)	Multiple attacks globally including hospitals, retailers' exfiltration + encryption, showing continued dominance of ransomware threats.
2024	Kadokawa & Niconico (Japan — media & video-sharing)	Ransomware / data-breach by threat-group BlackSuit: ~254,241 user records stolen.
2025	SimonMed Imaging (USA, medical-imaging provider)	Ransomware attack by Medusa data on ~1.27 million patients exposed (IDs, medical records, imaging data, etc.).
2025	Kering (owners of brands like Gucci, Balenciaga, Alexander McQueen)	Data breach by hacker-group Shiny Hunters customer personal data (names, emails, addresses, spending histories) of ~7.4 million customers exposed. No financial data stolen.

2025	Collins Aerospace — airport check-in & boarding software (vMUSE)	Cyberattack disrupted airport operations across several European airports; software

		compromise caused major travel disruption.
2025	City of St. Paul (Minnesota, USA)	Ransomware/coordinated cyberattack on municipal infrastructure led to state of emergency, National Guard deployed

Cybercrime has changed greatly over time, from being the early days of manipulating telegraph systems, all the way to large-scale attacks by ransomware and cyber warfare. One of the earliest versions of cybercrime occurred in 1834, when stocks were stolen from the French telegraph system. After that, telephone systems were disrupted for a number of reasons in 1878. The development of phone hacking (phone-phreaking) gained popularity in the 1950s, as individuals would use tones and sounds in order to manipulate the phone networks of their time. By the end of the 1960s, computers were being introduced into the community, which introduced an array of new ways for cyber criminals to infiltrate individuals and businesses. One example would be the 1969 RABBITS Virus; this was one of the first known instances of malware that could self-replicate. The emergence of digital financial crime took place in 1973 when a bank employee embezzled $2 million using computerized financial systems. By the 1980s, hacking became increasingly sophisticated; for example, Captain Zap's 1982 AT&T breach and the 1983 CIA-designed logic bomb that caused destruction of the Soviet Union's pipeline.

Levin caused global damage. In the 2000s, the explosion of enormous data breaches began, including the TJX data breach in 2006 and the Heartland Payment Systems data breach in 2008; these data breaches exposed millions of financial records. In 2010, Stuxnet was created as an online weapon that first damaged the machinery used in industry. The increasing use of online criminal activities for political reasons occurred in 2016 when the DNC was hacked, and in 2017, ransomware (e.g., WannaCry) caused chaos throughout the world. 2017 was also the year

when Equifax had a data breach and revealed how vulnerable companies with a lot of data stored within them can be. Critical infrastructure was also negatively affected in 2021 when Colonial Pipeline was attacked and disrupted the distribution of petroleum products throughout the US. The Kaseya attack in 2021 raised concerns about vulnerability of supply chains because many thousands of customers were impacted. While the disruption of essential services (including healthcare), and the recent disruptions of healthcare (Simon Med Imaging), and the aviation (Collins Aerospace) industries show that threats to national security and public safety will continue by 2025. Cyber-attacks are escalating to these essential services as well as financial institutions which are losing their digital assets (money) to other countries and foreign powers via cybercrime.

2.3 Cybercrime:

2.3.1 Characteristics of Cybercrime:

Main characteristics of cybercrime are as follows:

- Deliberately gaining unauthorized access to any computer system.
- Intercepting and damaging intentionally by deleting, deteriorating, altering, or suppressing of computer data without right.
- In a serious way by input, transmission, deletion, alteration, or suppression computer data.
- Producing, selling, procuring for distribution of equipment intended to carry out any of the aforementioned crimes or the use of passwords or comparable information to gain access to computer systems with the goal of carrying out any of the aforementioned crimes

2.3.2 Types of Cybercrime:

Cybercrimes are illegal activities mediated through the computers and electronic networks and though preparation of a crime is not an offence, the only emerging field wherein even preparation of a crime can also amount to an offence is Cybercrime which means if a person with an intention of intruding into the privacy of another person, intrudes into his private space by trying to access and hack his phone gallery and tries to change the data but later changes his mind, the said act still amounts to offence under Information Technology Act. Similarly, with an intention of helping other person or to save her from blackmailer tries to retrieve data without authorization, he is said to be liable under the said set of crimes without any exception. With the technological progress in all the countries, cybercrime rate is also increasing. Cybercrime

has two sides: on one side it relates to the person committing the crime and on the other side is the person who is a victim on whom the crime is committed.

Cybercrime or computer crimes can be categorized into two main classifications:

- A computer is a primary instrument for committing the crime, like theft, forgery, or pornographic actions. The computer was merely the tool used to commit the crime.
- The crime is done on a computer and its networks and software, like hacking into a security system, delivering a dangerous programmed, or infringement on a website title. Fig 2.1 represents the Classification of cybercrime. Classification of cybercrime are discussed below:

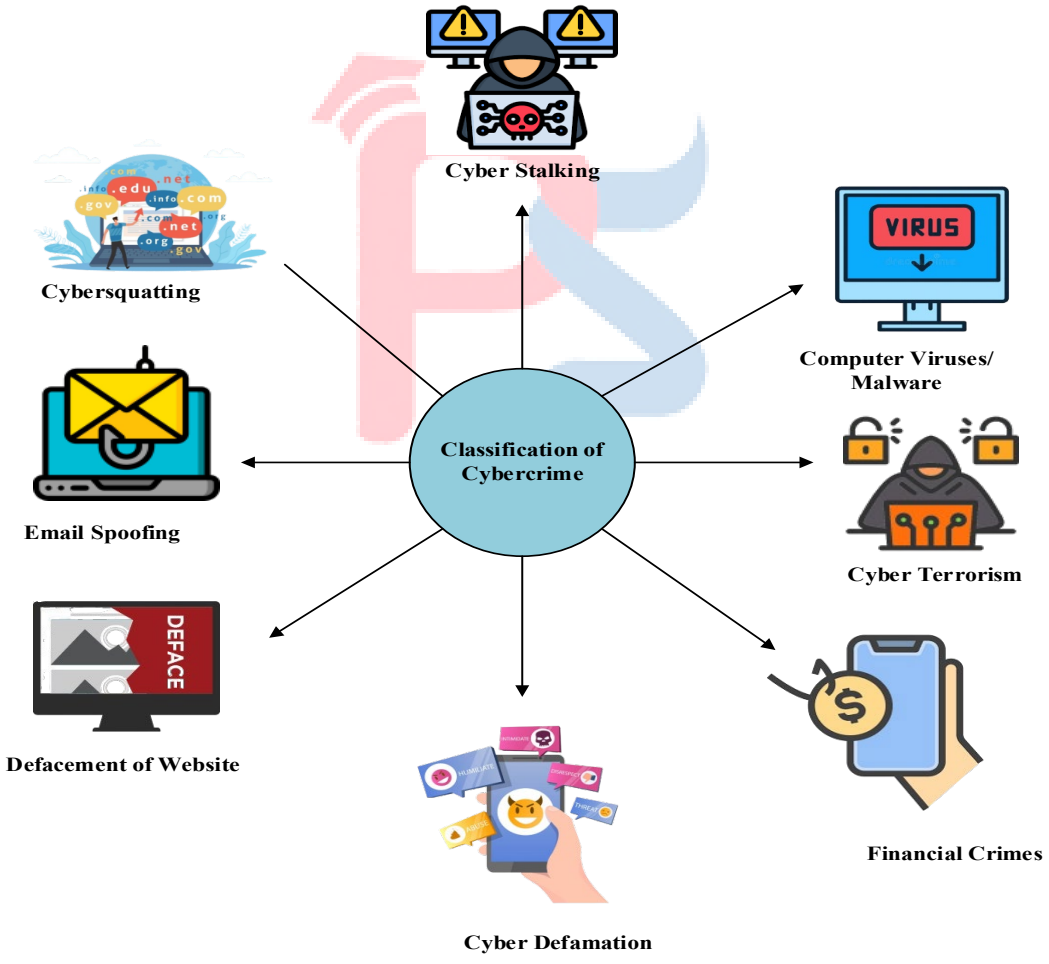

Fig 2. 1 Classification of Cybercrime

a. Cyber Defamation:

Cyber Defamation is a crime committed on cyberspace through internet, with defame someone. In this defamatory and derogatory matters about another individual is published on websites to injure their reputation. Defamation as an act and offence has been categorically defined in Section 499 of Indian Penal code while Section 500 deals with the punishment for same.

b. Cyber Stalking:

All forms of online harassment, including trolling, slander, defamation, false charges, and even direct threats to annoy, intimidate, frighten, control, or blackmail the victim, are included in the category of cyberstalking that the private information about the victim will be revealed over the internet. While a cyber stalker can be booked under both rely upon the legislative provisions as made out under various provisions of Information Technology Act.

c. Hacking:

The terms "hacking" or "hacker," we picture a clever person who attacks other computer systems, destroys them, cracks codes and passwords, transmits viruses, etc. They believe that computer "hackers" are crooks. They have a pessimistic attitude of the 'Hackers,' which is based on a misunderstanding. Computer thieves have been wrongly labelled "hackers" by the media in this instance. The term "hacker" has come to be associated with a negative meaning mostly because of the influence of the media. Erasing or deleting data from any computer resource with the aim to harm another individual or the public is a criminal offence. The civil liability depends on the amount of scam, criminal liabilities may be invoked as per Section 378123 of “Indian Penal Code and Section 75 of Information Technology Act”.

d. Defacement of website

When criminals gain access to a website and change its content, it's referred to as "web defacement" attacks. As a result of a hacker's intrusion, the comments might include political

and religious messages as well as obscenity and other unpleasant content which would embarrass the website's proprietors.

e. Email spoofing:

The way as active attacks like faking and Alteration of message contents. To make it appear as if the email was sent by someone else or from a different location, this technique involves modifying the sender's name in the email. Fig2.2 represents the email spoofing.

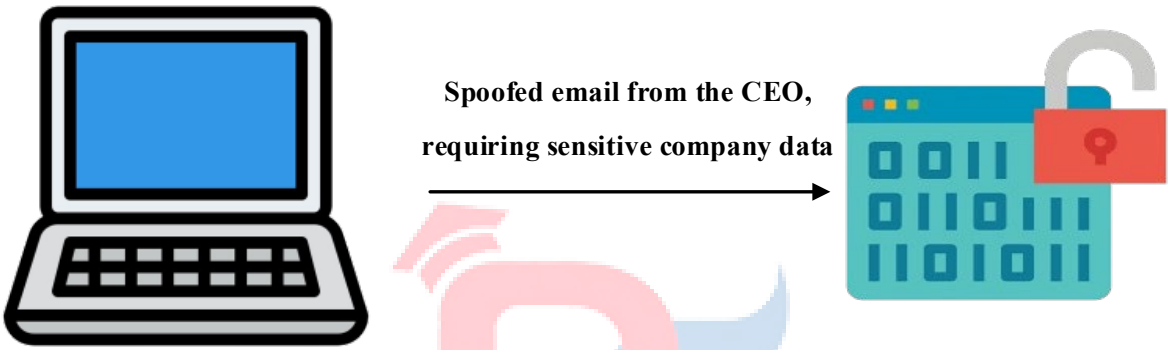

Fig 2. 2 Email Spoofing

The email is sent by the unauthorized person for stealing information through the email is called email spoofing. Spam attacks can be lessened with the right email server configuration & enhanced user knowledge of the issue, but they can still occur. The only practical preventative measure is the use of digitally signed emails.

f. Data Diddling

Data Diddling, is an illegal to change information before, during, or after it's been analyzed by a computer system, which is known as data tampering (DT) or data diddling (DD). During the writing process, recording, encoding, analyzing, verifying, translating, and transferring data, the original information can be affected by the person typing it or a virus designed to change it. It is regarded to be one of the most basic forms of computer crime**.**

g. salami attack:

The ancient "collect-the-round-off" method is used to slice salami. Mathematical routines, such as value computations, are used by the attacker. Calculations are done with decimal places, usually two or three

h. Computer Viruses/ malwares

Computer viruses are small programmed which are specially developed for corrupting or deleting data of a computer. Such viruses can be easily spread as email messages or attachments, if the attachment is opened the virus immediately gets downloaded and corrupts the programmed and data in the hard disk of that computer. Viruses are also spread when unauthorized software or files are downloaded from the internet. For example, Trojans are unauthorized programmer which may be a part of an authorized programmer, wherein a hacker may be using it to get someone's IP address and to hack that computer data remotely. There are many types of Trojans, some Trojans are destructive and may destroy the hard disk of the computer. There are also password Trojans which search for passwords in a computer system and sends it to the hacker via email.

i. Financial Crime:

These crimes have become more common because of the digitization and automation of financial systems. The fact that this crime was a coordinated, simultaneous attack on several banks made it noteworthy. Finally, a holistic strategy based on the same data and processes can be used to combine fraud, cybersecurity, and anti-money laundering (AML). Most of the benefits, however, will be available soon because of the merger of fraud and cyber operations .Fig 2.3 represents the financial crime.

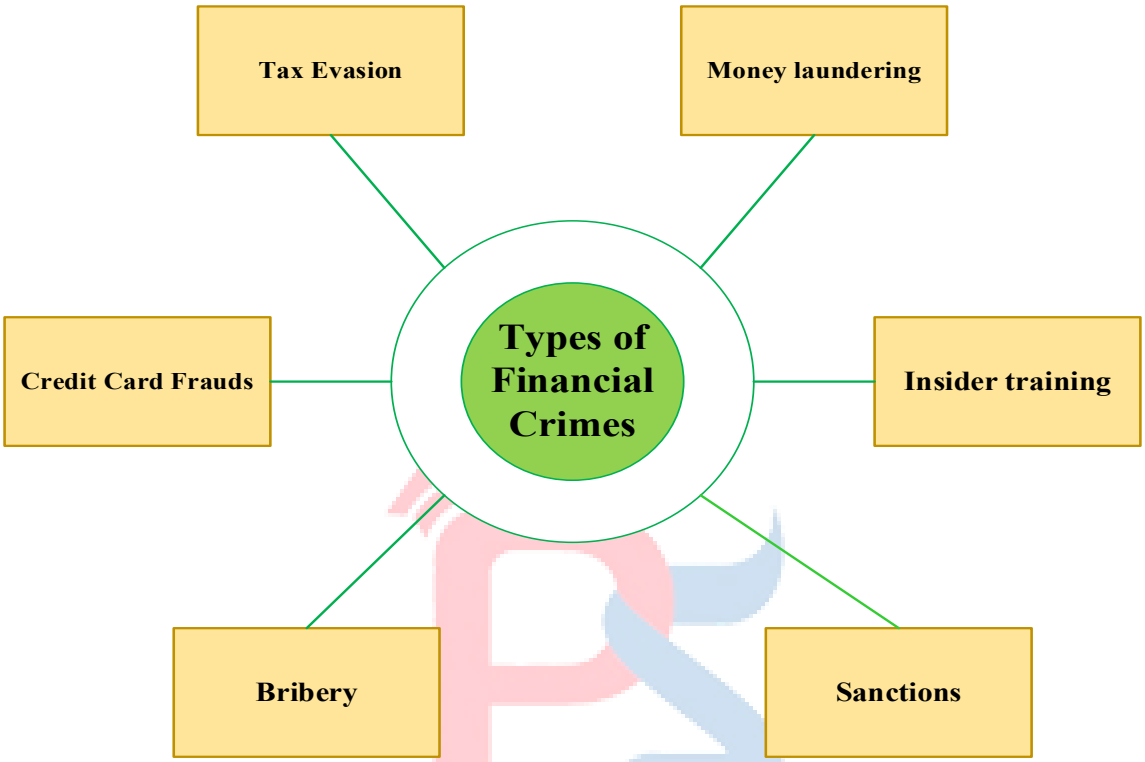

Fig 2. 3 Financial Crime

j. Web Jacking:

A cybercrime in which control of a website is taken over by force. The attackers do it for some monetary or political reasons. Once a web site is taken control then the actual owner of the website loses all his control, and the attacker will have full control of the website.

k. Cybersquatting:

The illegal registration, trafficking in, or use of a well-known web address with the goal of portraying it as being exclusive to the trademark owner with the intention of obtaining payment[18]

l. Cyber Terrorism:

The most dreaded of all the cybercrimes which is using disruptive activities or threats in cyber space intending to intimidate people for achieving religious, political, or social objectives. Individuals can interact with complete anonymity, rapidly and effectively across geographical borders, and to a practically limitless audience because of the Internet technological capabilities [18].

2.4 Evolution of Cyber Threats:

Evolution of cyber threats has mirrored rapid expansion of digital technology, becoming increasingly sophisticated and diversified over time. Initially, cyber-attacks were characterized by simple forms of malware and computer viruses, which primarily targeted individual systems to disrupt operations or achieve minor financial gains . The motivations (or reasons) to cause cybercrime in the early days were mainly out of curiosity or simply for the purpose of vandalism. However, as computer networks have expanded globally to become interconnected, the form and focus of Cybercrime has also become more complex.

2.4.1 Historical Development of Cyber Threats:

The twentieth century, many of the types of cyberattacks were simple computer viruses or worms. An example of an early example of a computer virus that had the ability to replicate itself in large networked environments is the Morris Worm that was created in 1988. It was through this worm that a significant level of disruption was accomplished as a result of a coordinated attack via the Internet. Table 2.2 represents Key Milestones in the Early Development of Cyber Threats. During the latter half of the 1990's and beginning of the 2000's many cyberattacks began to focus on extracting funds from individuals and businesses through the creation of online banking systems and e-commerce. Cybercriminals of that time began developing malware.

Table 2. 2 Key Milestones in the Early Development of Cyber Threats

Year	Event/Threat	Significance
1988	Morris worm	First major worm to exploit network vulnerabilities, causing widespread disruption
1999	Melissa Virus	One of the earliest email-based malware attacks, demonstrating the potential of spreading through user interaction
2000	Early Ransomware	Introduction of ransomware that demanded small ransoms for data decryption.
2013	CryptoLocker	A pivotal ransomware attack that marked the shift to large-scale, financially driven extortion.

2.4.2 Advanced Persistent Threats and State-Sponsored Attacks:

Advanced Persistent Threats (APTs) have grown out of the previously exploited opportunistic use of malware into a more sophisticated threat landscape that is built around long-term intrusions designed for espionage and sabatoge. APTs use targeted, coordinated and stealthy means to facilitate the infiltration and persistent presence within a target network over

an extended period of time. Many times, APTs are associated with state-sponsored actors that utilize APT threats to conduct attacks against the critical infrastructure, and multinational companies. APTs are highly sophisticated toolsets that implement sophisticated tooling and zero day exploits to circumvent conventional security measures and to allow for a long timeframe of undetectable presence within an affected network. Significant examples of APT include Stuxnet, which targeted Industrial Control Systems, while the SolarWinds breach utilized a compromised software supply chain to infiltrate and impact a wide range of organizations globally.

2.4.3 Emerging Threat Vectors:

Emerging technology continues to pose new threats to cybersecurity in today's marketplace. The growing number of connected Internet of Things (IoT) products, for example, has created significant security holes for both manufacturers and consumers alike. Many manufacturers do not provide foundational security features with their connected products, which makes them easy targets for the type of cyber-attack that an attacker who has gained access to an IoT device could use as a way to gain access to other parts of a network. Frequently, attacks against IoT devices form the basis for larger botnet attacks used by compromise that can be utilized to launch any number of other types of attacks, including Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

Along with leveraging the Internet of Things (IoT), some malicious attackers use Incorrect configuration of components or weak access credentials to gain unauthorized access to cloud-based systems. As evidenced by the rapid change in cyber-attacks, businesses todays must implement increasingly adaptable and scalable Security Solutions that provide Protection for growing, geographically dispersed and Changing networks.

Phishing attacks remain very popular today; however, as a consequence of AI (Artificial Intelligence) advances, they have also become more sophisticated and are becoming ever more common. Table 2.3 represents the threat vector challenges. For example, machine learning technologies now enable Phishing messages to be created using algorithms producing highly convincing messages designed to trick Users into revealing confidential "information" or downloading malicious software.

Table 2. 3 Threat Vector Challenges

Threat Vector	**Characteristics**	**Challenges**
IoT Exploits	Involves insecure IoT devices	Large attack surface, lack of standardized security protocols
Cloud Vulnerabilities	Targets Cloud misconfigurations	Complex infrastructure, remote access risks
AI-Enhanced Phishing	Uses Machine learning for customization	Difficult to detect due to high sophistication
State-Sponsored APTs	Long-term targeted operations	High stealth and use of zero-day exploits

2.4.4 The Need for Proactive and Adaptive Defenses:

Organizations should combine the use of proactive and reactive (flexible) defensive strategies to help combat the growing number of cyber threats faced by them on an ever-changing basis. Cybersecurity is powered by the introduction of AI (Artificial Intelligence) and ML (Machine Learning) technologies. These technologies enable rapid detection and response against incoming cyber threats through the rapid development

of new methods of detecting and mitigating the risks associated with these threats. In addition to these benefits, technological advancements also allow for a complete 24/7 monitoring solution, which will enable an organization to see all events occurring within its operating environment, discover anomalies, and automate preventative measures. All of these advantages contribute towards the increased resilience of the organization and ultimately create a dynamic adaptive security posture.

Coordinating efforts to collaborate internationally with all stakeholders and sharing intelligence related to cyber threats are both fundamental components of a strong defense posture. By working together, the government and the private sector will facilitate the detection and mitigation of new threats, while improving the overall cyber resilience of all organizations. As organizations prepare security strategies for the emerging threats that will arise during the 21st century, it is essential that they remain current with the evolving technologies being utilized by attackers and develop flexible and scalable solutions [19].

2.5 Technological Developments Shaping Cybercrime

Cybercriminals have increased their arsenal of tools and techniques that are available for their use, and they also have been able to expand the geographic "attack surface" area of their attacks. Therefore, as technology continues to evolve, we will see increasingly sophisticated and automated types of cyberattacks that will have devastating real-world impacts.

Privacy-Enhancing Technologies (PETs):

Establishing a government's accountability for its cyber activity is extremely challenging, and therefore requires very substantial proof to satisfy international legal standards. This creates a legal and political sensitivity around cross-border attribution.

The collection and analysis of large volumes of personally identifiable information (PII) makes a large number of those data points available for illegal or fraud; due to this volume of

information, when criminal breaches are established, it will affect millions of people with potential identity theft/fraud activity.

Cryptocurrencies and Blockchain:

Certain cryptocurrencies anonymity makes it easier for money laundering, dark web transactions, and cyber extortion (such as ransomware payments), which makes it challenging for law authorities to trace financial transactions.

Cloud Computing and Data Storage:

The increasing dependence on cloud services for data management and storage creates new risks. Inadequately configured cloud settings and “application vulnerabilities” can lead to large-scale “data breaches, unauthorized access, and operational disruptions”.

Internet of Things (IoT):

Smart homes, wearables, and industrial systems are just a few examples of the numerous interconnected gadgets that increase the "attack surface." Due to the poor security of many IoT devices, hackers can gain access to household or corporate networks, steal data, or initiate other assaults.

Artificial Intelligence (AI) and Machine Learning (ML):

Cybercriminals utilize artificial intelligence to conduct automated attacks, produce extremely authentic-looking phishing email messages, and develop hyper-realistic digital likenesses of people of video and audio for use in impersonating individuals or perpetrating fraud or disseminating false information. AI-enabled bots may also be leveraged by cybercriminals in massive DDoS attacks and to propagate false information[20].

2.6 Privacy, Data Protection and Digital Identity:

“Privacy, Data Protection and Digital Identity” defines the safeguarding of individuals’ personal information and online identities from unauthorized access, misuse, or surveillance in digital environments

2.6.1 Privacy as a legal and human right:

Privacy refers “fundamental human right” which protects an “individual's autonomy”, independence and dignity from unwarranted infringements. It is also considered to be an individual's right to control sensitive information and determine when, how and to whom that information will be collected, utilized or distributed. Thus, because of the rapid increase in the number and types of personal information that individuals create, store and process through the use of information technology and communications, privacy has become an increasingly important issue in modern society.

Legally, the protection of personal freedom and the sanctity of human dignity are closely linked to privacy. Privacy is a contract between the government and private companies that no unreasonable interference with someone's life, communications, or any aspect of their personal information (i.e., medical records, employment history, etc.) exists. Privacy also protects the fundamental principles of democracy and supports society's adherence to the rule of law by preventing unwarranted surveillance, profiling, and misuse of personal data [21].

“Human rights” are essential to every human, irrespective of personal traits. They are unalienable moral rights that predate all laws and cannot be granted or taken away by others. When one has these rights, life takes on meaning. Man cannot exist without it. One specific topic of discussion is the protection of human rights under the criminal justice system. The term Human Rights indicates both their nature and their source. Human beings are rational beings. They have certain essential and inalienable rights, commonly referred to as human rights,

simply by virtue of being human. These rights do not come from being a citizen of a particular state; rather, they are a part of who they are and are based on the qualities of human nature. During criminal proceedings, law enforcement agents violate the majority of human rights. One of the most important aspects of human rights worldwide is the criminal justice system. The criminal justice system is one area of the legal system where it is necessary to priorities maintaining social order and public safety. However, it is important to consider how to uphold the human dignity of both the accused and the victims of the crime. Men are social creatures by nature, and they coexist with other people in civil society. As a result, society has emerged and regulations governing its members' behaviour have been established. The association serves a variety of human life goals in addition to providing friendship. Conflicts of any form can inevitably occur from interactions between members of the community. The criminal justice system is one of the ways that each government uses its own adjudication process to resolve any type of issue. Research on the criminal justice system is extensive. Custodial jurisprudence, accused jurisprudence. There are always crimes.

A civilization without crime did not exist. To manage crime and create a society free from crime, the government enacts penal laws. Law is not a ghost without a home. It necessitates a social home. Laws should be written in a way that allows victims of crime to get compensation and perpetrators to be punished. Both Bangladesh and India have their own statutory and constitutional criminal jurisprudence to carry out individual justice. Despite the fact that human rights have been discussed and written about extensively over the ages, it is still difficult to define the phrase. However, as one author has brilliantly noted, "Human rights may be difficult to define but impossible to ignore". It is a dynamic notion that strives to adapt to the demands of the day. Because of this, the term's definition and meaning are heavily influenced by the circumstances and viewpoints that are prevalent in a certain civilization at a particular moment, and it takes on new dimensions as history progresses. The form and content of human rights are always evolving, as is the socioeconomic context in which the issue of human rights is inextricably linked. Therefore, it is impossible to define human rights in a way that is universally applicable. Human happiness and the complete development of the human

personality depend on human rights. They are essential to the advancement of humanity both mentally and physically. These rights are unalienable because the community's enlightened conscience would not allow anyone to give them up, not even voluntarily. In addition to being essential for the formation of the human personality, these rights are unalienable because without them, humans would be degraded to the status of animals. These rights, which are founded on the fundamental material and immaterial needs of life, are a statement of what a life is at the very least worthwhile. Naturally, there can't be a single viewpoint on what constitutes a minimally worthwhile life, basic needs, and, consequently, human rights. However, several rights such as "the right to a dignified life, the right to freedom of conscience, and, of course, the right to a decent standard of living"—must still be considered fundamental. Human rights are founded on humanity's growing desire for a respectable, civilized existence where each person's inherent dignity is upheld. Fig 2.4 represents the Human rights. It can be categorized into three main categories:

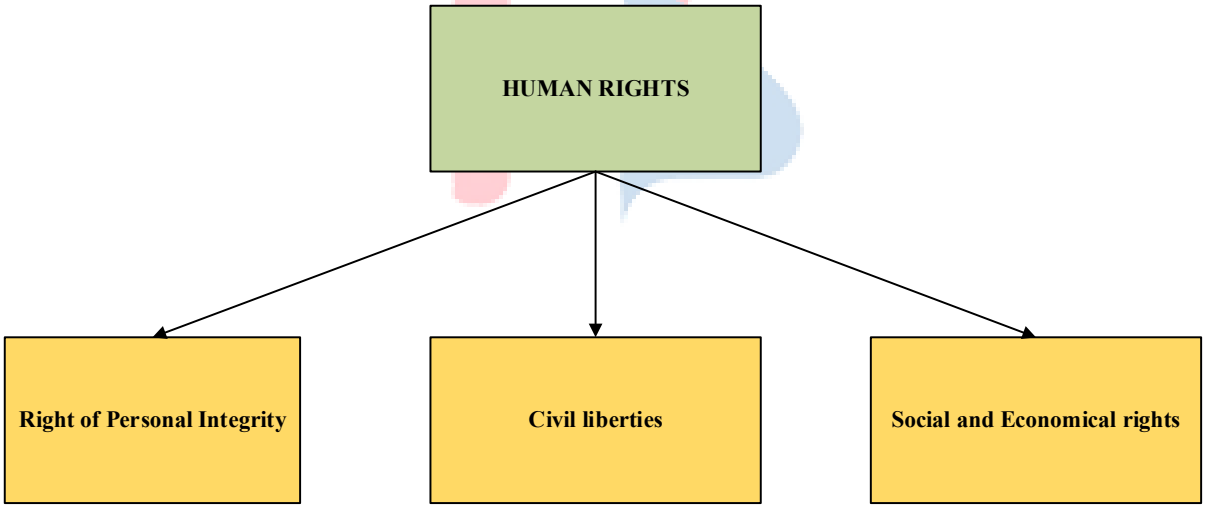

Fig 2. 4 Human Rights

Right of Personal Integrity: It guarantees that no one is subjected to torture, cruel treatment, or unlawful interference with their body or mind. It is based on human dignity and includes freedom from coercion and consent in medical situations. It is essential for both individual autonomy and larger societal justice.

Civil liberties: Civil freedoms include the ability to verbally and physically express one's ideas. These rights include the freedom of speech, thought, conscience, and religion. Additional civic rights include the capacity to vote, run for office, get married, and start a family. Civil liberties protect people from governmental interference and enable them to enjoy personal autonomy with regard to their views, opinions, and actions, provided that the exercise of such rights does not injure another person. The Constitution (which includes the U.S. Bill of Rights) includes these rights: freedom of speech; of religion; of the press; of assembly; of privacy; of a fair trial; of no unreasonable searches and seizures. Civil liberties differ from civil rights that deals primarily with elimination of discrimination based upon race or color.

Social and Economic rights: Social and economic rights involve basic human needs and rights of development. These include right to food, shelter, medical care, education and right to work. Socio-economic rights are a group of human rights that provide individuals with access to adequate living conditions, well-being, and dignity. These rights cover basic needs such as housing, food, healthcare, education, and employment, as well as social security, which requires governments to act positively (progressively realize) to meet these needs. In contrast, civil rights primarily require governments to refrain from interfering with individuals' personal freedoms and liberties. Socio-economic rights are intended to ensure that individuals have all of the resources and conditions necessary to live decently and are therefore fundamental to promoting both freedom and equality through addressing the inequitable distribution of wealth in society.

Internationally, privacy has been recognized as a human right under various legal instruments. Fig 2.5 represents essential human rights. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights prohibit arbitrary interference with privacy, family, home, or correspondence. The concept that privacy is a fundamental right of humanity and that privacy can be accessed regardless of country or technology is expressed in many governmental constitutional provisions.

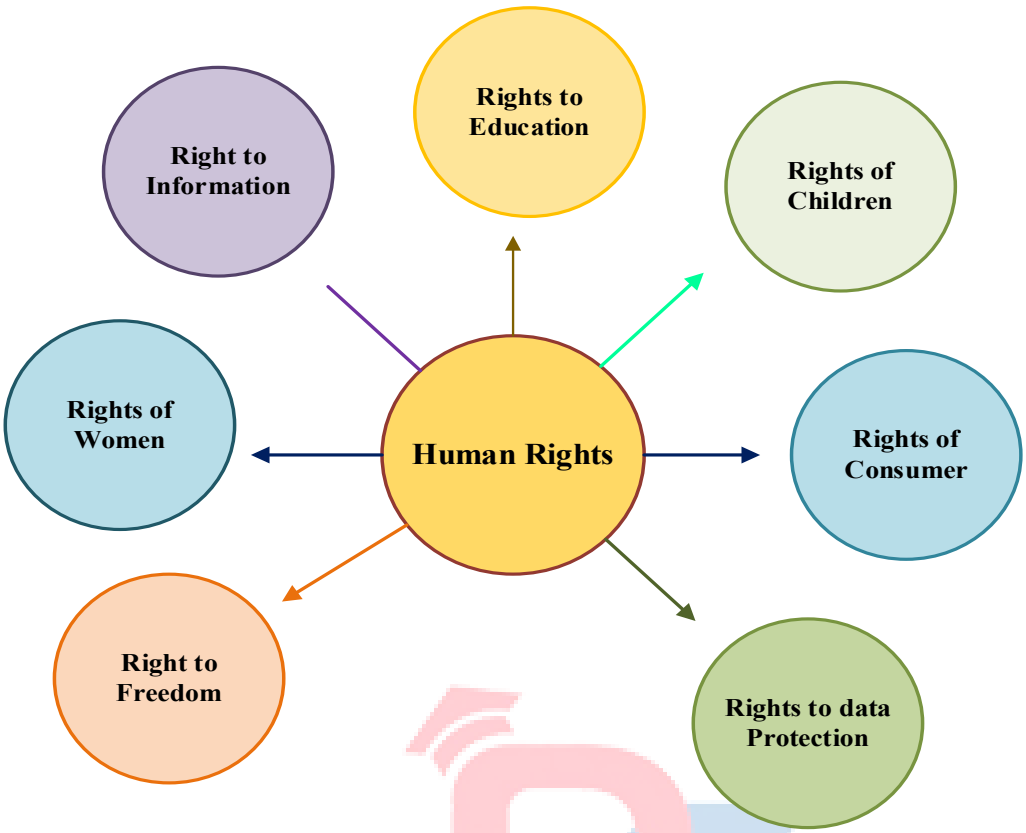

Fig 2. 5 Essential Human Rights

In the realm of cybersecurity/digital governance, privacy has equal significance as it has been highlighted by concerns of government-sponsored mass surveillance, the exploitation of personal data without use, the rising popularity of biometric technology, data analytics and AI and additional emerging surveillance technology. The provision of security and assurance of privacy legally protects all technical advancements using various means available to prevent the dangerous and illegal exploitation of personal information, as well as the protection of people from potential harm caused by these same types of technology.

Privacy exists as a legal right and therefore obligates government to both positively and negatively uphold and protect it. While a state's responsibility is to refrain from unnecessary interference with personal life on the negative side, on the positive side it should enact laws and create mechanisms that assist in protecting individuals from violations of their right to privacy by private entities. The responsibility is practically fulfilled through privacy protection laws

and protections, processes for providing consent, and measures holding private organizations accountable for violating individuals' rights to privacy.

Privacy is a legal and human right that serves as the foundation for balancing the rights of an individual with the rights of society and the national security of a national entity. It ensures that measures taken in the name of security, public order, or technological progress remain proportionate, lawful, and respectful of human dignity. Thus, privacy remains a cornerstone of democratic societies in the digital era [22].

2.6.2 Data protection principles:

2.6.2.1 Data Protection:

"Data protection" defines "a collection of privacy regulations", guidelines, and practices designed to reduce "privacy violations" brought on by the "gathering, storing, and sharing of personal information". In this context, "personal data" refers to "any information or data that speaks about an individual and can be used to identify that individual". Typically, the government, any commercial company, or an agency will gather such data or information. In other terms, data protection is a system talking about the security of data from any unauthorized accessed. Different methodologies and levels of data protection are used by individuals, corporations, and governments. In this data-driven environment, corporate organizations and huge corporations started recognizing data as an asset. They also recognized value in the distribution, collection, and storage of data. To achieve this goal, they started protecting their massive data. Since the right to privacy, which includes "personal data, is a fundamental right in India", the Indian government must enact and implement legislation for the protection of personal data.

It requires particular legislation with severe penalties and a redressal system to counteract the growing number of cyberattacks, including identity theft and data theft. Since the "right to privacy", which includes data privacy, is a fundamental right in India, data protection is a right. Furthermore, without data protection, no data privacy is feasible. Data protection is therefore a

right as well. Data property is an essential source of income and can only be taken away with due procedure. Compensation under Article 21 may be sought if someone violates the same. Everyone has the right to possess and enjoy their property under Article 300A of the Constitution. Therefore, a person's property cannot be taken away from them unless the law permits it. Both tangible and intangible properties are included in the expressiveness property. Data property would also fall under the definition of property under Article 300A. Therefore, if an individual's data property is breached or misused, this article will be violated. Without going too far with the idea of monetizing personal data, it is also possible to treat personal data as valuable property. In exchange for consent to use their personal data for specific purposes, data subjects may receive valuable returns like rebates or other incentives. The phrase is commonly used to describe the effort to create systems with human-like cognitive abilities, including as the capacity for reasoning, meaning-making, generalization, and experience-based learning.

Goal of artificial intelligence, a subset of computer technology, is to enable machines to perform tasks intelligently, much like humans would. Artificial intelligence, to put it briefly, is the capacity of a machine to think and behave like a human or to mimic "cognitive"10 functions that people connect with other human minds. Legal system came into being after the country's social structure underwent a protracted evolution. Without laws and regulations, society cannot function. Anarchy will result from a society without norms. The Vedic era is when the legal system's history begins. Because he didn't understand the concept of society, the man was initially like an animal. Man, then realized that society was necessary since without it, his interests could not be protected. After man embraced the culture, he socialized and society was born. The idea of culture emerged when people realized that basic needs could not be met without it. Therefore, culture was created to help man meet his requirements. Humans, society, and their culture all grow up together, and the entire spectrum of cultures in the various societies is similar and closely related. Man's quest for justice began as soon as he entered society. Conflicts of interest among all members of the community led to the necessity of a justice delivery system. The issue of how to resolve conflicts of interest among society's members now

comes up. Balancing the interests of members and society as a whole is the finest approach that has been chosen and is still in use. In another sense, good human relations are necessary to resolve individual disputes [23].

2.6.2.2 Data protection principles:

Some of data protection principles and they are:

- Lawfulness, equity , and openness
- Limitation On Purpose
- Data reduction
- Accuracy
- Storage Constraints
- Integrity and secrecy
- Accountability

Lawfulness, equity and openness:

"Lawful" refers to “collection and processing of data with a legitimate legal foundation”. One popular method of establishing a “legal basis for processing personal data is to gain the user's consent”. The GDPR and other data regimes provide numerous legal justifications for processing personal data. When process personal data in a way that is both in the best interests of the individual it pertains to and that the individual may fairly anticipate the extent of the processing, are being fair. This should be done in a style that makes it simple for the persons handles the data to the extent and techniques of processing.

Limitation on Purpose:

In this concept, it only use “personal data for the intended use”. It shouldn't use personal information for unrelated purposes.

Data Reduction:

In this principle, it shouldn't gather more personal data than is required to deliver the service. Alternatively, merely gather and examine the exact amount of information needed. Fig 2.6 presents Data protection principles

Accuracy:

The goal of the approach is to have the most precise data possible. To make sure of that, the controller and/or processor should take "reasonable measures". But this is pertinent when the correctness of the personal information matters to the individual.

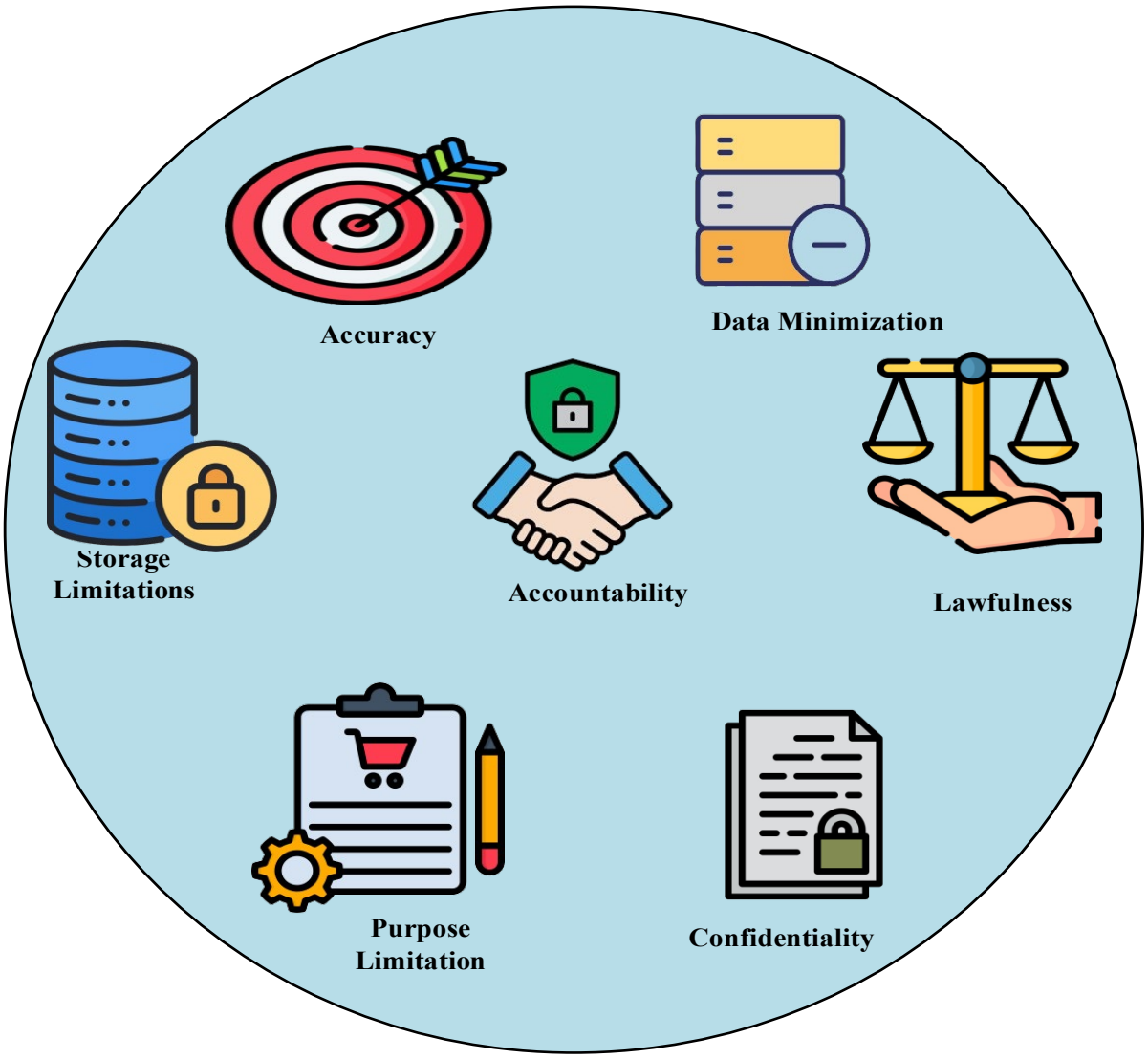

Fig 2. 6 Data protection principles

Storage constraints :

It states that when personal information is no longer needed, it should be deleted. If personal information is no longer required for the intended purpose, it should not be retained. Many businesses view the elimination of outdated data as a component of the data minimization principle, which is closely related to this idea. to create a secure data removal method to guarantee that data that is no longer needed is really deleted and isn't kept on a device or in the cloud, where it might pose a security risk.

Integrity and secrecy:

Integrity is ensuring that personal information is accurate and unchangeable by third parties (to protect the systems against hackers). Ensuring that only that access the personal data are processing it is the essence of confidentiality.

Accountability:

The accountability with accepting accountability for the way data is processed. It suggests that the data controller and/or processor are in charge of ensuring that personal data is processed correctly and in accordance with the regulations [24].

2.6.3 Digital identity, anonymity, and exploitation

The Digital identity referring to the activities, and expression and experiences of individuals exhibited in online spaces [25]. The phrase "digital identity" is often used in the growing body of research on "identity theft." The protection of personal identities on the Internet is one of the two challenges that any discussion of digital identity must clearly address. We start by noting that the process necessary to ascertain a person's identity is sometimes called "authentication" or "identity verification." When the process is mostly computer-automated, the term "electronic identification" is commonly employed [26]. The digital identity system can be classified as three types and they are: Centralized, Federated, and Decentralized. A "digital identity" is an online persona that an individual constructs in cyberspace. A digital identity employs digital identifiers like an email address, domain name, or URL to identify its holder, just way the information on a passport identifies its owner for a specific purpose.

. These days, applications for business services, Personalized services, and government services save and modify user personal data. On the internet, user digital identities are still kept in central repositories under the control of unauthorized third parties who alter and remove user data. This becomes a concern since identity theft, security theft, etc. may occur, necessitating the use of extremely aggressive solutions. Digital identity is a huge, worldwide problem that requires attention. Because of the existence of digital identities and the individuals who use them, entity management has emerged as one of the most important issues in this Internet age. Due to their extensive use of the Internet and its services, the majority of people nowadays have some kind of digital identity. Fig 2.7 represents types of digital identity . Because users must remember many passwords to access multiple websites, the methods are effective.

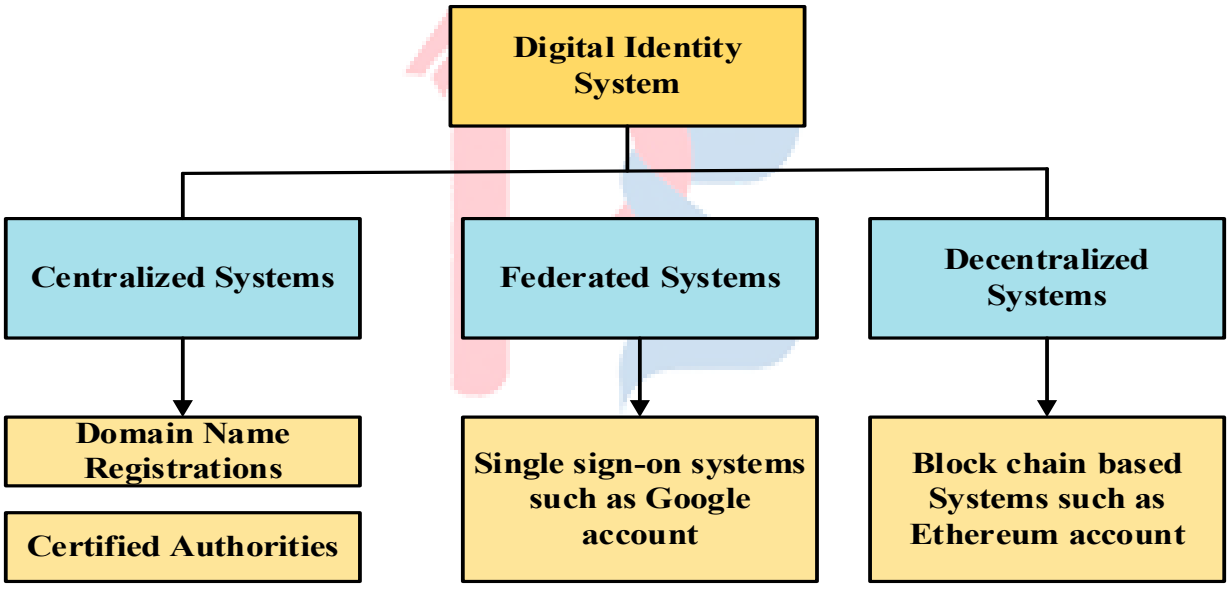

Fig 2. 7 Types of Digital Identity

A “central Identity Provider (IdP) “is in charge of gathering, creating, and maintaining identity data from entities in centralized identity systems, such domain name registrations or certificate authorities, where all activities take place in one setting. Although companies may benefit greatly from centralized identification systems, maintaining several accounts across various service providers has become challenging. To facilitate mutual confidence between two or more centralized identification systems, a Federated identification Management (FIM) solution is suggested.

This authentication technique, often known as federated Single Sign-On (SSO), allows entities to securely enter into several applications using a single identity. The capacity of the owner to establish, maintain, and delete identity components from any place at any time is referred to as identity management. The identity must be under the owner's control since it is existential. However, because large amounts of data are centrally held and only a few parties, or IdPs, have control over it, the entire identification system is very vulnerable under centralized and federated models. Decentralized identity based on blockchain provides a novel solution to these problems. Due to its independence from a central authority and potential to provide all the aspects of federated identity, it represents a breakthrough in the field of digital identity management. For instance, profiles linked to the state administration, with which personal data (including address, taxes, mobile phone number, social security numbers, or individual identifiers) would be shared, are examples of data and their generated profiles. Other private profiles could be associated with companies such as banks or retail stores; in this case, the data will include the actual transactions, such as contracts for credit cards, savings products, payments, personal addresses for product delivery, and previous purchases. Last but not least, the audience will learn a lot about the acting persona from the person's posts on social media, blogs, forums, and other platforms. These activities will make a significant part of their online profile and disclose a lot of information to third parties. There are eight application and competence levels listed under "Digital Identity Management." It merely defines digital identity management, acknowledges the data used to create it, and suggests sophisticated solutions, such managing a business's online reputation [27].

2.6.3.1 Digital identity management:

The Internet's architecture enables users to conceal their online identities, which has led to a search for trustworthy methods of definitively determining identities. Identity tokens must be tamper-resistant, or challenging to fabricate once they are granted, in order to guarantee that data subjects are clearly identified. Therefore, the need for parties to be present during

transactions and interactions is eliminated by digital identification. Personal information is disseminated more widely as a result of this disembodiment of identifying processes. Cameron suggested the rules of identity as design principles that ought to serve as the basis for identity construction. Fig 2.8 presents Two Phases of Digital Identity scheme. According to the study, following these guidelines gives users authority over how their personal data is utilized for secondary reasons. When these design principles are not followed, users become concerned, which may affect how they interact on social media.

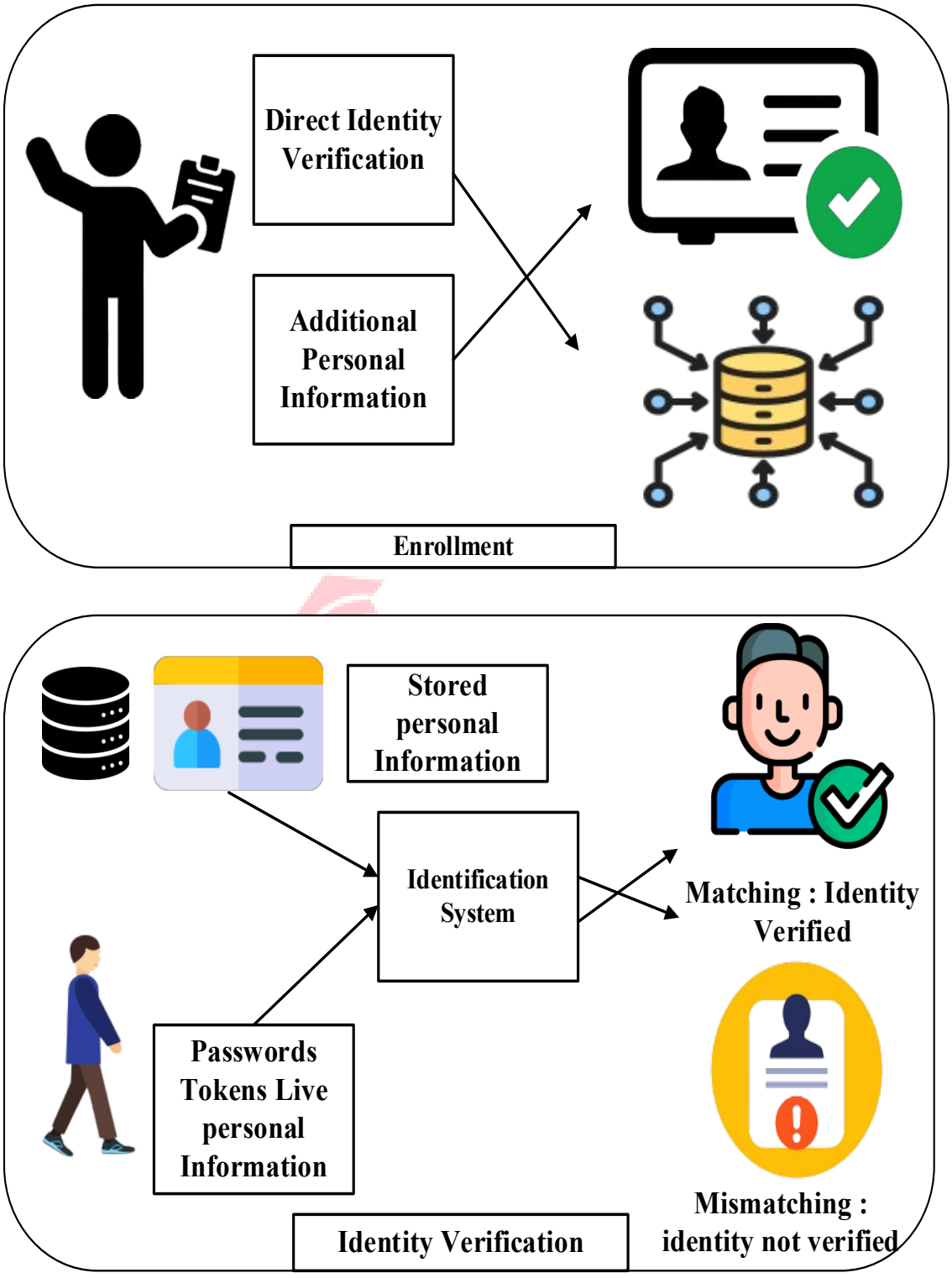

Fig 2. 8 Two Phases of Digital Identity scheme

2.6.3.2 Self-Sovereign Identity (SSI):

SSI is a novel "user-centric model of digital identification that puts the identity owner at the centre of digital identity control without requiring a third party". It is based on claims and proofs. In SSI, a claim is a statement made by an entity that something is true. The blockchain serves as a substitute for the registration authority in centralized/federated systems, known as Registry. It is predicated on the Issuer's user-specific attributes. The proof shows that a computational truth is true and is either an argument or cryptographic evidence. To put it another way, the proof supports the assertions. Assets are moved off the blockchain (off-chain) for anonymity, and the genuine identity claim is kept in a user-controlled area, usually in a cryptography network. The publicly accessible identifier and the identifier in the user's submitted claim can be compared by a verifier. Technically speaking, SSI relies on the utilisation of DIDs. In order to create a framework for signing and validating credentials and integrating with "DIDs, W3C" has published several drafts of Verifiable Credentials (VCs), since DIDs are merely foundation identifiers of decentralised identity that serve as a starting step in characterizing their subjects. Consequently, VCs are a collection of claims that enable the entity to authenticate and/or authorize another entity without the requirement for a central authority or third parties throughout the authorization. They also cryptographically demonstrate who issued them. An identity must be transportable and not limited to a particular site, supplier, or location in order to be considered self-sovereign.

An ecosystem that facilitates the acquisition and recording of attributes as well as the spread of trust across entities utilising these identities can help enable such mobility. Technologies derived from fundamental ideas in identity management, distributed computing, blockchain, and cryptography form the core of SSI. Open standards and protocols like W3C-established decentralised identifiers (DIDs) and verifiable credentials (VCs) should be followed by SSI solutions. Fig 2.9 generated Self-Sovereign Identity. The core tenet of SSI is that people have authority over their data and, thus, sovereignty over their digital identities. This idea is what sets SSI apart from earlier identification models that saw people as users. Under this new approach, sovereign persons decided[28].

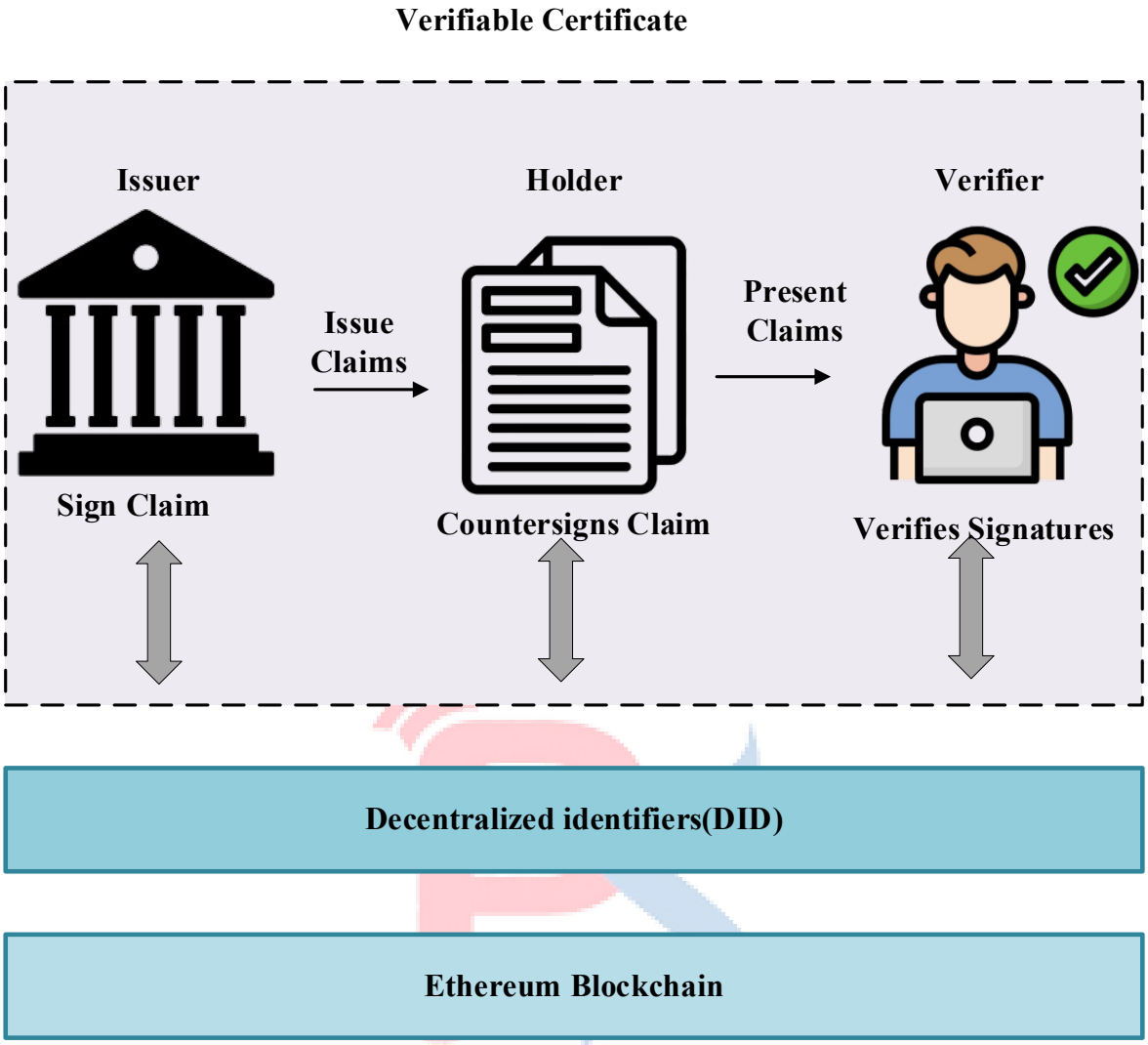

Fig 2. 9 Self-Sovereign Identity

2.6.3.3 Privacy Challenges in Digital Society

Privacy challenges in the digital society refer to the difficulties in protecting individual's personal data and informational autonomy in an environment dominated by digital technologies, online platforms, data-driven services, and constant connectivity. The problems caused by large-scale collection of data, the use of surveillance technologies, user ignorance, cyber risks, the failure of regulatory bodies to enforce regulations and the misuse of sensitive "information by public and private entities" will increase as more digital contacts are created, making it increasingly complicated to maintain confidentiality, obtain permission and control over one's own personal information.

From a legal perspective, the ineffectiveness of current laws and enforcement mechanisms to address issues of abuse of collected data, monitoring and movement of collected data across borders, and digital violations of “the right to privacy” are considered to be privacy issues in today's digital society. Advanced technologies such as “Artificial Intelligence, Big Data Analytics, Cloud Computing and the Internet of Things (IOT)” provide privacy issues in today's digital world through the ability to collect process and create profiles of large amounts of data beyond control of individuals. The ethical problems related to consent, transparency, autonomy, and the power imbalance between digital platforms and individuals (who provide their data to these platforms) are some of the factors that negatively impact human freedom and trust in the digital world today. Fig 2.10 represents privacy challenges in Digital society.Other privacy issues in the digital age include cyber-attacks, data breaches, identity theft, to an individual’s information, which put both privacy and personal safety at risk in the course of digital communications [29].

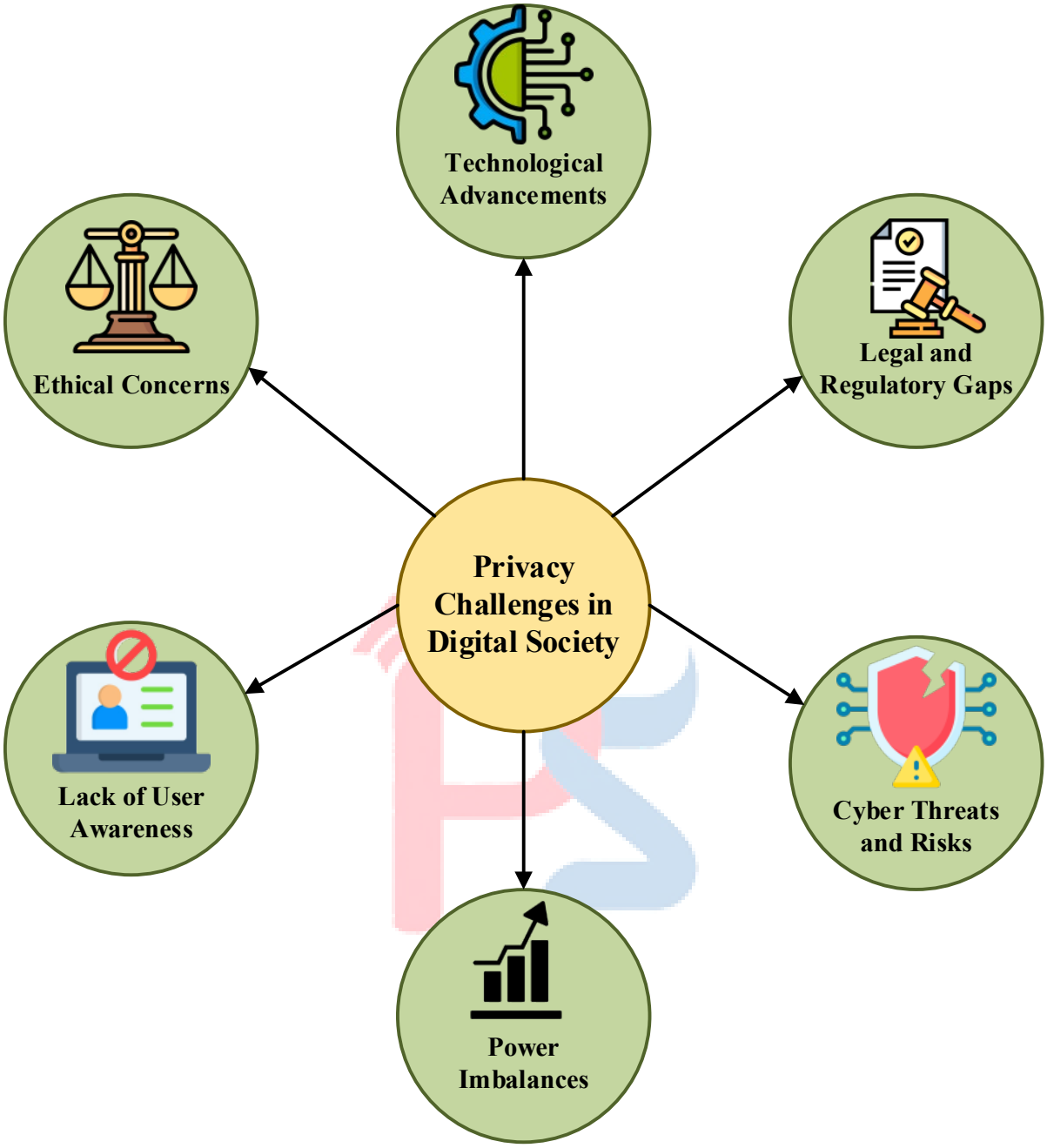

Fig 2. 10 privacy challenges in Digital society

2.7 Cyber Surveillance and Civil Liberties:

2.7.1 Cyber surveillance and its evolution:

Surveillance has been used by powerful rulers and governments for ages for purpose of collecting “personal information” about targeted sections of the population. The information gathered by surveillants can be harvested and used in a variety of ways. Such personal information has proven particularly helpful to warring nations in knowing the personalities of both their allies and adversaries and keeping out for potential covert plots against them. Surveillants view cyber surveillance as a potent instrument for learning more about their targets. Cyber surveillance systems are designed to capture the enormous volume of digital footprints left behind by the daily activities (e.g., banking, shopping, education, and entertainment) and communications (e.g., social media interactions, email communications, and video conferences) of internet users from internet-connected systems. These digital footprints give the surveillants useful information that may be essential for figuring out the targeted people's interests and creating behavioural profiles, as well as for determining the type of interpersonal interactions. It goes without saying that surveillants also have access to a vast amount of communication data that contain private information about their targets, such as social media login credentials. By deploying spyware to compromise and snoop on internet-connected systems, such as end-user devices (such as smartphones, and IoT devices), cyber surveillance systems can gather this data remotely. Cyber surveillance tactics are more covert than previous methods since they don't require the surveillants to physically access their targets' devices (Cybersecurity and Infrastructure Security Agency, 2019). These days, a surveillant can watch their target's keystrokes from anywhere in the world by remotely installing keylogger software on their system. The extent to which powerful governments continue to conduct widespread cyber surveillance, frequently without their citizens' knowledge, was made clear by the 2013 Snowden disclosures (Macaskill and Dance, 2013). Communication records, financial data,

social and economic position, political affiliation and links, and relationships between different segments of the population are a few examples of personal information gathered by surveillance. Government surveillance programs have always been a contentious issue. This is mostly because citizens don't have complete faith in the government, there is a lack of transparency about the data gathered, and there is doubt about how the data will be used. For example, when the Singaporean government disclosed that surveillance data gathered to track Covid cases had been shared with the police to support criminal investigations, the people of Singapore were extremely alarmed. Additionally, when a surveillant is covert, as is the case with network monitoring, citizens become even more alarmed. For example, Kazakhstani civilians were unaware for about a year that their government had been working with a large ISP to intercept all of their online communications. Not only do governments benefit from network surveillance, but private organizations like corporations do as well. Big businesses frequently want to keep an eye on the amount of traffic that their rivals' websites receive. This is due to the fact that an examination of traffic volume trends gives these businesses important information about how well they are performing in comparison to their rivals and aids in their comprehension of the requirements and inclinations of the target consumer groups. Cybercriminals frequently employ network surveillance to disrupt citizens lives for their own gain or to cause financial damage to businesses. Network surveillance is frequently used by cybercriminals as a prelude to more significant operations. In order to perform a denial-of-service attack when the server is busiest, a cyber attacker might, for example, track the amount of traffic sent to a banking server over time to determine the server's peak load time. This would enable the attacker to increase the attack's impact. Internet consumers now view network spying as a major security and privacy threat because of the aforementioned issues. This has driven the necessity for protecting information shared via the internet.

2.7.2 History of Cyber Surveillance:

In an 4th century BCE, when Indian and Chinese emperors relied on in-person espionage for their military intelligence (Yuen, 2014; Mazhar Abbas, 2021). The target of the surveillance could vary from a high-profile individual to a group of ordinary citizens. For instance, surveillance was extensively used by the USA during the First World War for identifying domestic insurgents (BBC, 2019). Even today, surveillance is widely used by developed nations for governance and in warfare. Over the years, surveillance techniques have become increasingly sophisticated and evolved from labor-intensive in-person espionage to wiretapping (1895) (Pollak, 2015), monitoring radio communications (circa 1917) (United States Army, 1991), followed by digital techniques (circa 1960) (Spillane, 2022), and cyber surveillance (circa 1986) (Sentinel One, 2019; Edwards, 2020)[30].

2.7.3 Balance between state protection and civil liberties:

The civil liberties in India, as this study aims to do, is at once a historical question as well as one that implicates the present, each of which has a bearing on our efforts to critically thematize transformations in the public sphere. It is historical in that the idea of civil liberties was important to certain public forms of claims-making in India, with contorted to suit the needs of its disparate protagonists.

2.8 Legal Theories, Cyber Governance and Norms:

2.8.1 Applicable legal theories:

2.8.1.1 Security–Liberty Theory

The Security–Liberty Theory is founded on the inherent tension between the State's obligation to ensure national security and its duty to protect individual liberties, particularly privacy and freedom of expression. While this perspective accepts "the need for security to protect" society against such as "terrorism, cybercrime and cyber warfare", it also recognises that excessive security. The timeliness and pertinence of this debate is intensified within cyberspace due in large part to the extensive surveillance capability available through such technologies as interception of data, monitoring of online communications and collection of bulk data.

In many instances, Governments use the concepts of national security, supported by evidence of a threat posed by terrorists, to warrant the use of invasive cybersecurity tactics based on the justification of protecting public order, protecting cyberspace from the threat of cyber-attacks and ensuring that citizens' private information is safe from exposure or misuse. However, these justifications should be considered seriously in terms of accountability, necessity and proportionality. The Security-Liberty Theory thus identifies a need for a balanced legal system that combines adequate protections (assessment by the courts, open government records, and experience and respect for the constitutional framework) with all security procedures. Hence, the Security-Liberty Theory creates an avenue to assess whether the current cybersecurity policy and/or surveillance laws provide a reasonable balance between protecting an individual's liberty and society's collective security needs while at the same time preventing excessive sacrifice of individual liberties in the name of increased security [31].

2.8.1.2 Risk Regulation Theory

Risk regulation theory is based on the recognition that society has become increasingly vulnerable to complex and often technology-introduced risks. The inherent complexity of technology-related risks means they will never be completely eliminated and must be specifically managed. This includes the growing range of digital risks caused by information technology and global cyberspace connectivity such as cyber-attacks, identity theft, and/or data breaches; as well as newer and more serious types of digital risk, such as the use of cyber terrorism. This view advocates using legislation not just as an instrument of harm after the fact but also as a way to anticipate, assess, and manage these digital risks.

To enhance the likelihood of cyber-attack occurrence and their effect, Risk Regulation Theory advocates for the application of preventative legislation(s) in the area of Cybersecurity. Examples include Data Protection Standards, Compliance Regulations, Cybersecurity Audits, and Proactive Monitoring. Furthermore, Risk Regulation Theory endorses the use of the "Precautionary Principle" as a basis for taking regulatory action to mitigate the effects of Cyber-Attacks where there may be an unacceptable risk (hazard) associated with them, especially when that risk has not been sufficiently identified.

An example of an evolving concept in cybercrime that has created a shift from taking a reactive approach to a more proactive model of crime control is the manner in which cybercrime law uses the risk regulation theory as a means of governing the areas of resilience, risk mitigation, and institutional preparedness. On a more specific level, by utilizing the prevention, accountability, and adaptive regulation concepts, risk regulation theory will enhance our understanding of current cybercrime laws. Current cybercrime laws are intended to provide some limits on the risk that new technologies pose to our economic stability, public trust, and innovations, while minimizing any constraints on future technology development or the profitability of new technology [32].

2.8.1.3 Digital Constitutionalism:

The idea at the core of risk regulation theory is that complex, tech-related dangers are increasingly appearing in today's world, so we can't eliminate them completely; we have to manage them properly. Examples of risks coming from digital systems and international connectivity in cyberspace are identity theft, computer hacking, data breaches, and Cyber terrorism. The philosophy behind this approach is not just to react to damage after it has occurred, but also to be able to use the law as a means to anticipate, assess, and regulate those risks. There are many ways that the Digital Constitution has been put into practice legally. Examples of this are the many different kinds of laws that protect people's information from problems caused by companies through issues like privacy and security. Digital Constitutionalism also provides guidelines for how laws related to high-tech advances and National Security Policy should be structured so they align with the principles of the Constitution; it establishes that all laws regarding the Digital World must protect people's rights, be proportional to their needs, allow for accountability and recognize that society has a duty to respect individuals' rights to live with dignity [33].

2.8.2 Cyber governance frameworks:

In addition to the framework of international agreements, plans, laws, policies, guidelines, and standards that operate, cyber governance is the process of making decisions that promote accountability, transparency, and involvement in activities linked to cyberspace best together. One of the most important topics in international relations these days is cyber governance. International organisations have looked for answers to the problems associated with cyber governance. The "private sector, civil society, and the public sector" which includes "political organisations and public sector organizations" are all included in governance.

One of the actors in this process is public organisations, which concentrate on how to better serve their citizens. By upholding the rule of law, controlling socioeconomic conditions, building social and physical infrastructures, and establishing social security nets, governance

sets the foundation for equality, peace, and justice. As the second actor, the private sector includes private companies across a range of industries.

The creation of jobs and revenue streams, the development of production, trade, and human resources, as well as via the supply of services and corporate standards, these organisations guarantee economic growth and development. Multistakeholder governance models were analysed and recommendations for their enhancement were made in cyber governance research. These improvements include granting financial resources to empower marginalised stakeholders, equitably distributing leadership positions, and increasing decision-making transparency with a veto restriction. It has been said that both official and informal methods must be used to regulate cyberspace. [34].

Cyber Governance Challenges:

- Some of the challenges are faced by the Cyber governance are:
- Rapid Technological Advances
- Resource constraints
- Compliance Complexity
- Cultural Resistance

Rapid Technological advances:

Due to their rapid advances, technology provides unprecedented levels of difficulty in addressing governance of cyberspace. Technologies are expanding the "attack surface" exponentially, making it easier for hackers to compromise systems. Technology also increases the complexity of threat vectors and outgrows our ability to build effective regulatory and legal frameworks to counter new threats.

Resource Constraints:

Effective cyberspace governance is seriously challenged by the limitations imposed by constrained resources in relation to gaps in the areas of technical abilities, such as the need for qualified cybersecurity employees; capital investment; and the utilization of current technology to ensure safe cyber operations.

Compliance complexity:

The evolution of cyber threats and technologies has created an intricate web of complex compliance problems for governance (cyber compliance) due to many competing regulations that often overlap/conflict with one another (ex: GDPR and PCI DSS). SMEs are often ill-equipped to meet the demand for timely updates on compliance requirements (due to resource restrictions), require multiple technologies to support their operations and processes, face increasing numbers of suppliers/sells of products or services, and struggle to maintain an effective GRC program. As a result of these challenges, there exists a disconnect between "checking-the-box" compliance and actual security and, therefore, there exists the need for organizations to have a more proactive and integrated approach to building their GRC strategy, rather than relying solely on compliance.

Cultural Resistance:

The impediments to effective cyber governance presented by cultural resistance are extensive. They encompass a vast array of human, individual and group, and organisational impediments to the adoption of secure behaviours. Challenges arising from cultural resistance to cyber governance are occurring on many levels throughout organizations and at the geo-political level .Fig 2.11 presents Cybersecurity Governance steps.

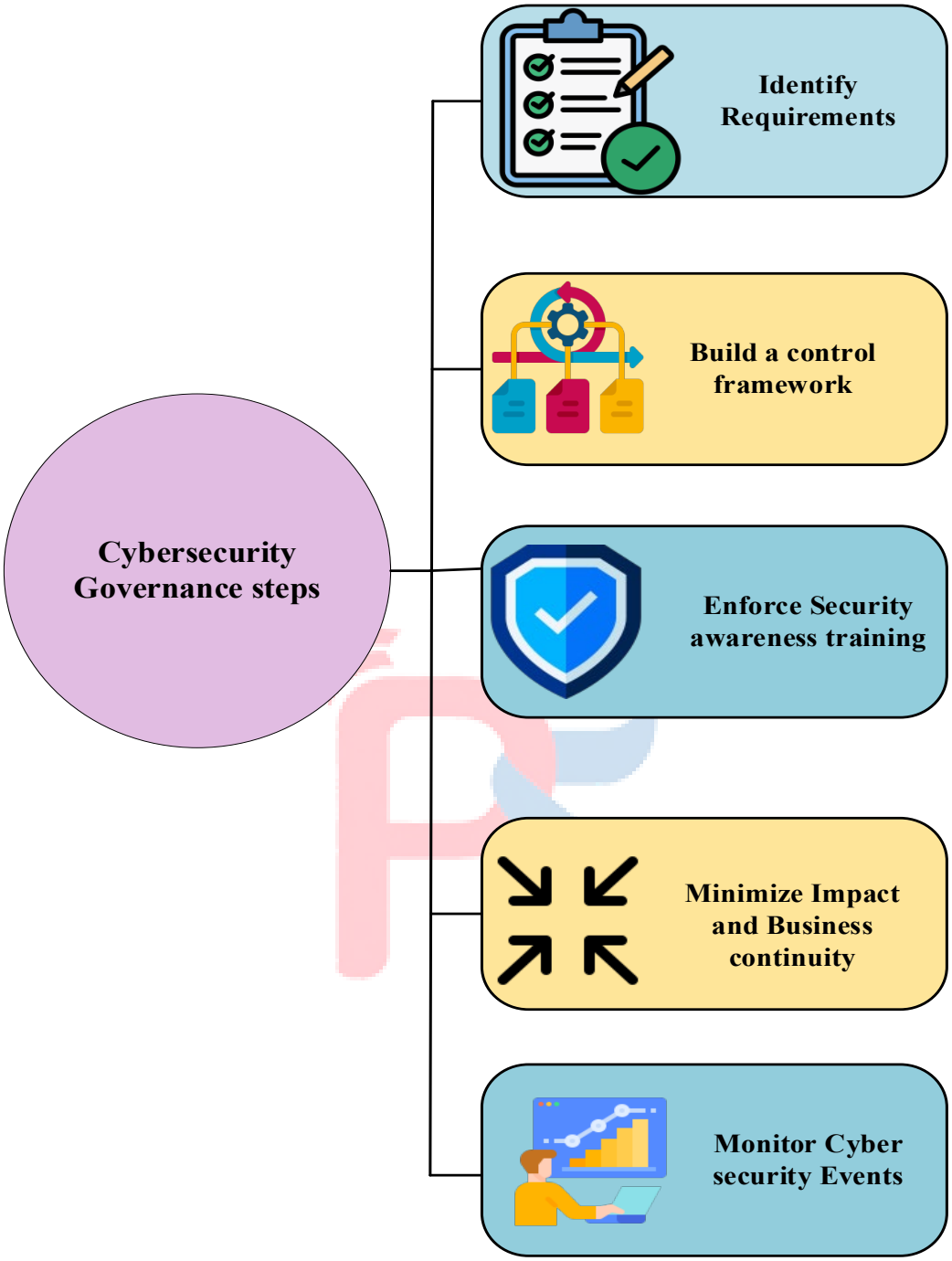

Fig 2. 11 Cybersecurity Governance steps

Identify Requirements:

Cybersecurity goals can be defined with the use of organisational objectives. Determine the strategic goals and align your security objectives with them in collaboration with stakeholders and leadership.

Build a control framework:

The next step is to build controls in accordance with the defined requirements. These controls will confirm that the governance rules are being followed by all of your company's assets people, vendors, devices, infrastructure, risks, and policies.

Enforce security and awareness training:

The training should be provided and enforces as a security.

Minimize Impact and Business continuity:

To ensure business continuity and lessen the effects of cyber disasters, governance is essential. It entails identifying events, reacting to them, resolving them, and recording them for future reference.

Monitor Cybersecurity events:

Control monitoring should also involve modifying your cyber security procedures to stay up with evolving market norms and threat landscapes. To safeguard your system from contemporary threats, you might need to update your policies.

Cybersecurity governance process category:

External:

There are many types of factors used to assess whether an organisation's cyber-security practices meet acceptable standards; some of these are based on established industry standards, others on established laws and regulations, while still others are determined by "industry best practice". All three of these categories of factors will influence the Organization’s decision-making process regarding its cyber security.

Financial:

For an organization to successfully implement the critical success factors, both the Organization itself and any of its third-party partners must have a strong level of cyber security to provide total security. Fig 2.12 Cybersecurity process category. In general, the organization's financial resources determine whether or not it will be able to allocate funds to support its financial cyber-security measures. Therefore, both the adoption factors relating to the organization's financial cyber-security and the Critical Success Factors to be implemented will be dependent upon the capacity of the organization to install and maintain the cyber-security measures effectively.

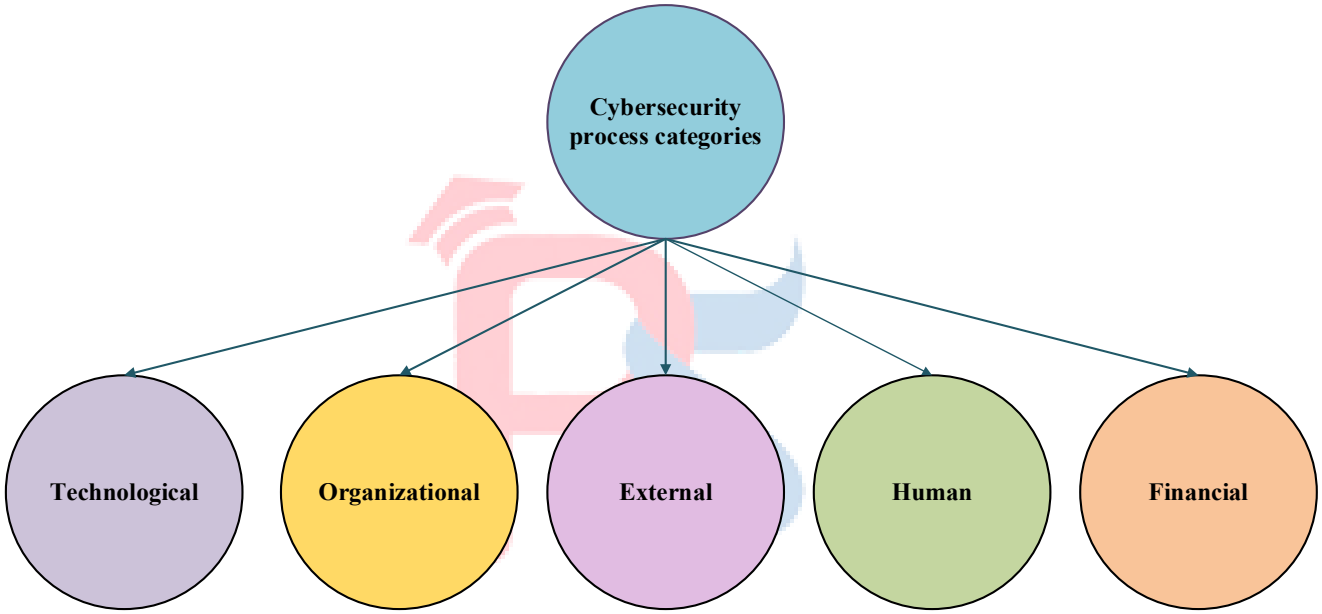

Fig 2. 12 Cybersecurity Process category

Organizational:

This process area includes customer needs, business continuity, cybersecurity governance, and company reputation. Organizational processes are a very broad and complex topic that affects many aspects of business operations.

Technological:

This relates to the technological concerns that influence choices regarding the adoption and application of cybersecurity. Therefore, it includes the technical aspects of choices about the purchase, implementation, and ongoing upkeep of cybersecurity systems and

technologies. Included is a cybersecurity evaluation of the company's whole IT portfolio [35].

2.8.3 Cybercrime norms:

In this term broadly encompasses the legal frameworks, regulations, and statutes that govern and address issues arising in cyberspace, including the internet, digital communications, and electronic transaction.

2.8.3.1 Introduction to Cybercrime Norms:

Cyber law, often known as internet law or digital law, is a broad field that includes a variety of legal precepts, rules, and case law that regulate activities carried out online. It covers the legal ramifications of a number of online activities, such as “digital communications, electronic commerce, intellectual property rights, privacy issues, cybersecurity, and freedom of expression”. Cyber law is intrinsically multidisciplinary, incorporating ideas from both specialized fields like technology law and information security law as well as more conventional legal subjects like criminal law, contract law, intellectual property law, international law, and constitutional law. The key focus of cyber law is to create legal norms, rights and responsibilities that govern cyber space, which is a virtual world created by the connection of many computer networks together.

There are no geographical boundaries in this virtual world, and therefore traditional legal concepts, terms and definitions don't apply and as a result are constantly being called into dispute. Thus, in this worldwide digital marketplace, cyber law will help establish the rights and responsibilities of digital users, businesses and governments. Cyber law also covers a broad range of issues associated with the use of digital technology and online applications. To achieve the regulation of e-commerce, for example, cyber law provides a framework for electronic signatures, electronic contracts, consumer protection, and electronic payment systems. Additionally, cyber law covers an individuals or businesses' digital intellectual property rights to include copyright, trademark, patent, and trade secret protection against infringement and

piracy occurring in cyberspace. To protect the privacy of individuals and their personal information from excessive digital monitoring and data collection that now occur on a global scale, cyber law has established legal frameworks for personal data privacy including requirements for consent, notification of data breaches, and the transfer of personal information across borders to protect the individual's right to privacy in cyberspace.

Also, Cyber Crime and Cyber Security are based on Cyber Law. Cyber Law outlines many of the criminal offenses that happen within cyberspace, such as Hacking, Intentional spreading of viruses, Identity Theft, Online Fraud and Cyber Terrorism; It provides the mechanism to prosecute Hackers and prevent and penalize hostile acts. The Cyber Law establishes minimum Cyber Security standards, mandates the timely reporting of breaches to Cyber Security, and sets guidelines for all entities to comply with regulations to reduce the risk of Cyber Attacks on Critical Infrastructure, Digital Assets and Sensitive Data.

In addition to establishing the guidelines, standards, and enforcement mechanisms to allow the digital ecosystem to function seamlessly, Cyber Law is an integral component of the broader Legal Framework that governs activity in “Cyberspace”.

2.8.3.2 Significance of Cybercrime norms in digital age:

As cyberspace increasingly influences nearly all areas of modern society, the growth of cyber law has been profound. With billions around the world considering cyberspace part of their daily routine – from social networks to e-mail to shopping and banking – the actions, responsibilities, and interactions between citizens, corporations, and governments in cyberspace are directly impacted by cyberspace law. The Main goals of Cyber Law is to create laws and regulations that “govern online conduct and protect users’ rights and interests”; Cyber Law encompasses broad areas, including but not limited to: Data Privacy; Cybersecurity; Cyber Defamation; Copyright and Patent Infringement; and Criminal Activity Online. Cyber Law provides the framework for offenders to be held accountable, protects confidential information, and enables users to trust the online world.

Moreover, cyber legislation facilitates cooperation and collaboration between countries faced with global cyber threats and challenges. Because cyber security and law enforcement require transnational cooperation from all levels of government, law enforcement and the private sector, it is imperative to establish a framework through the development of a coordinated global response to cyber events; give global access to threat intelligence; and provide uniformity in legal standards and procedures. Cyber law thus provides the legal frameworks, principles and procedures necessary to govern the behaviour of individuals and businesses in the virtual world. The “legal environment for Digital Age” will continue to become increasingly important as societies around the world are faced with new challenges that threaten to erode their basic rights, interests and security. It is imperative that as cyberspace evolves and creates new issues, laws and regulations pertaining to Cyber.

2.8.3.3 Need for Cybercrime norms:

The number of unsettling incidents that occur frequently in cyberspace, such as identity theft, terrorist attacks, and money laundering Because of its anonymous nature, it is feasible for them to engage in a wide range of illicit activities without fear of repercussions. To maintain criminal activities in cyberspace, individuals, businesses, other entities of a similar kind and taking advantage of these "grey areas," which has resulted in the necessity of enacting cyberlaws[36].

2.8.3.4 Importance of Cybercrime norms:

One of the reasons why cyber laws are so prevalent is that they comprise a significant amount, if not all, of the activities and transactions that take place over the internet. It is possible to have the impression that cybersecurity affects every technical area, and it is also possible to believe that they have no influence on the activities that take place in cybersecurity. According to the theory, the reality is that every activity and action that takes place in cybersecurity is related to some legal and/or cyber legal protections, regardless of whether or not this effect is there.

Issues and Difficulties to enforcement of Cybercrimes:

Cybercriminals are developing strategies to circumvent international measures aimed at resolving the issue. Fig 2.13 presents, issues and difficulties of cybercrime. Here, the challenges faced by humanity that contribute to persistent cybercrimes are discussed as follows:

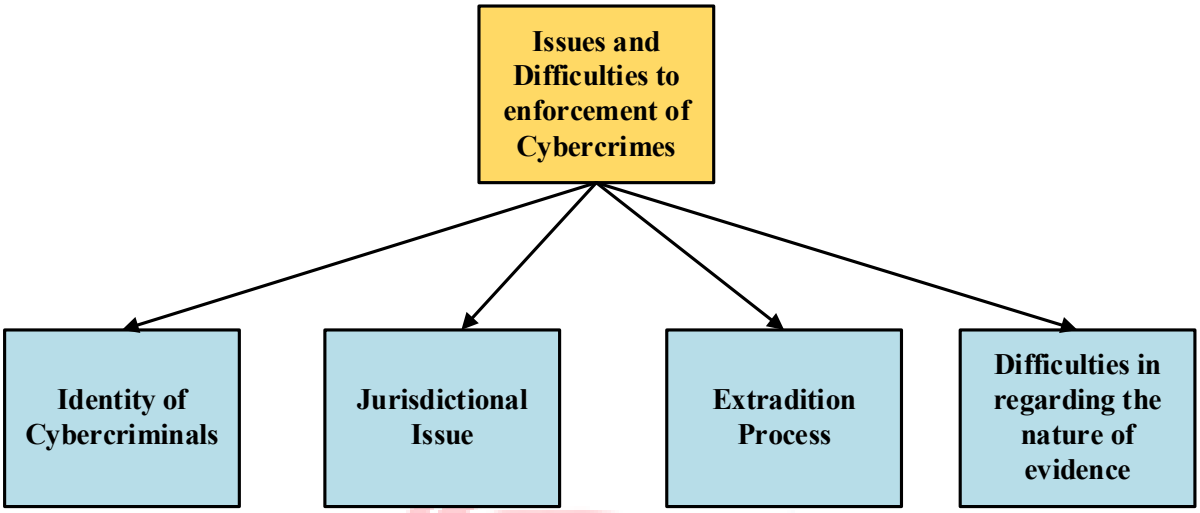

Fig 2. 13 Issues and Difficulties of Cybercrimes

Jurisdictional Issue:

The worldwide scope of cybercrime makes jurisdiction a difficult topic to settle. On the other hand, section 75 discusses how the legislation operates outside of its borders. It will only be meaningful, though, if it recognizes court rulings and information orders issued by qualified authorities that are not within their purview. Ward could be defined as a court's or judge's level of engagement in a certain activity, request, or procedure. The ward issue in the Alade v. Alemu Loke case is so radical that it delves into the fundamental underpinnings of any problem and becomes the basis of any mediation. If a court needs a location, it also needs to be fit to try the case. Because the methods are invalid and void stomach muscle initio, a deformity in capability is fatal. In any event, the case may be guided and highly selected.

Extradition Process:

The term "removal," you are likely hearing a combination of two French words, ex and custom. It is a step in rehabilitating a criminal suspect by an alternate legitimate expert for preliminary or discipline.

Difficulties in regarding the nature of evidence:

One other obstruction to the requirement of cybercrime laws any place endeavors are made anyplace over the globe, is the idea of proof accessible in the care of indictment and the acceptability of same, during the course preliminary of cybercriminals. What frequently demonstrates the existence of a reality is the proof. Declarations, authentic proof, narrative proof, and other evidence may be presented as needed. The law of proof contains all of the standards governing the admission of facts and verifications in proceedings under the close supervision of a court, with special attention given to the rules governing the acceptability of proof and the exclusionary rules.

Comparative National Security Strategies in Cyberspace:

Considering security in the broadest sense for every individual in the community is the aim of a certain social system or society's security structure. Thus, the foundation of the national security system is the structural relationships between security and human needs. The concept of using a security system to provide protection has existed throughout human history and is still prevalent in contemporary societies. The efficacy of a state's national security system ensures the safety of its population in the contemporary global order. The effectiveness of this machinery is represented by the countries' capacity to guarantee social progress and the welfare of their residents, as well as their capacity to protect their fundamental social ideals from both internal and external threats.

Despite having different perspectives on how states and the world function, the realism place particular focus on two factors: national interest and national power. The two relevant factors that determine the state's NSS are national power and national interest. Since India's national interest may differ from state to state, it must be made explicit. National security comprises a wide range of policies, including defense, maritime, technological, and nuclear power, since there are many components of “national power, such as military build-up, defense acquisitions, and technology level”. Nonetheless, the research concentrates on two essential tactics: nuclear and defensive. Defense strategies are essential since they are a nation's first line of defense in

times of conflict and war. Nuclear strategy grew in significance as nuclear power developed and progressed [37].

The following core values reflect national interests:

- Safeguarding the national sovereignty of India
- Protecting countries territorial integrity
- Preserving India's legitimate position
- Increasing the capacity in every facet of security
- Maintaining the legal and constitutionally guaranteed territorial integrity of land, sea, and air, including island territories.
- settling territorial and border disputes with India's neighbors.
- Protecting the lives and property of Indian citizens during periods of terrorist attacks and uprising.
- Keeping up a strong nuclear deterrent to prevent the use or threat of nuclear weapons against India
- Defending military command and control systems and vital infrastructure from cyberattacks by state and non-state actors and creating offensive cyber operations capabilities to prevent such strikes.

“After World War II”, “concept of national security” generally changed. While James Madison's writings and, more recently, Hans Morgenthau's works contain elements of the contemporary concept of national security, 1788Morgenthau, 1948). According to “Walter Lippmann (1943)”, “a nation feels secure when it is not pressured to accept legitimate interests in order to avoid war and when it is able to protect these interests through war, if challenged” (Lippmann 1943). Preventing physical damage is only one aspect of the concept of national security; It also relates to preserving states' legitimacy, avoiding losses that can compromise fundamental values, and defending vital political and economic interests. To defend various

aspects of their societies from external or internal threats, leaders strive to establish or preserve national security [37].

2.9 Jurisdictional and Cross-Border Challenges

2.9.1 Juridical concepts

The juridical concept of cross-border crime is grounded in principles of criminal jurisdiction that determine a state's authority to legislate, adjudicate, and enforce law. Traditional legal systems rely heavily on territorial boundaries, which become increasingly inadequate when criminal conduct transcends national borders.

2.9.1.1 Principle of Territorial Jurisdiction

The idea of geographical jurisdiction is central to criminal law. States are able to control crimes committed inside their borders thanks to territorial jurisdiction. However, with cross-border or multi-jurisdictional criminal behaviour, where the preparation, execution and effect of a criminal incident take place in several locations or states, the application of this principle becomes complicated, leading to a system of fragmented legal authority.

2.9.1.2 Principle of Nationality

The nationality principle permits states to claim jurisdiction over an offender or victim based upon their nationality or citizenship. The nationality principle is frequently used when a national of a particular state commits a crime in a different country or suffers harm as a result of a crime committed in a foreign country. However, the reliance upon the principle of nationality creates jurisdictional conflict when multiple states claim jurisdiction over the same crime at the same time.

2.9.1.3 Protective and Effects Doctrine

Through the protective principle, states assert jurisdiction over acts performed outside their boundaries if such acts have an impact on their National Security or are important to their vital interests. The effects doctrine asserts a state can claim jurisdiction over any crime that occurred outside of its boundaries and created significant consequences within its territory. The

protective principle and the effects doctrine have significant relevance to Cyber Enabled Cross-Border Crimes. However, both principles are very controversial due to their extraterritorial application.

2.9.1.4 Universal Jurisdiction

Universal Jurisdiction Universal jurisdiction permits all states to prosecute serious-specific crimes, independent of the jurisdiction where the crime occurred or what nationality the perpetrator or victim is from. Historically speaking, universal jurisdiction has only been applied to crimes like piracy, genocide, and there are still questions as to whether it can also apply to serious transnational cybercrime

2.9.1.5 Jurisdictional Conflicts and Forum Selection

Jurisdiction Conflicts and Forum Shopping Jurisdictional overlap between states frequently leads to conflicts, including forum-shopping, duplicative prosecutions, and diplomatic disagreements. Clear rules on how to select a forum for cross-border crime would create stability in the resolution of these cases

2.9.2 Attribution and cross-border issues

Attribution describes how to identify and legally connect criminal activity to a particular actor. In the context of cross-border crime involving digital technology, attribution encompasses both technical and legal aspects.

2.9.2.1 Technical Attribution Challenges

Technical attribution refers to tracing digital activity back to its source through the use of technology, including TCP/IP addresses, server logs, and network analysis tools. Anonymization techniques, proxy servers, encryption, and botnets significantly reduce the ability to accurately traceback the source of digital activity using technical means.

2.9.2.2 Legal Attribution and Evidentiary Standards

The standards of evidence recognised by courts pertaining to technical evidence must be satisfied to establish legal attachment to a digital content. Discrepancies regarding these standards in each country create difficulties utilizing cross-border data in criminal matters.

2.9.2.3 Role of Intermediaries and Third-Party Actors

The involvement of third parties (e.g., ISPs, cloud/proxy services, and social media) makes it challenging to determine the liability of these entities and their obligation to cooperate (if any) because they may operate in various countries.

2.9.2.4 Jurisdictional Barriers to Attribution

There are jurisdictional impediments when locating evidence/servers/suspects in foreign territories. As a result of lengthy procedures to obtain MLATs and letters rogatory, there is a possibility that once the necessary documents are obtained, the volatile nature of digital evidence may result in a less comprehensive case than originally intended.

2.9.2.5 State Responsibility and Cross-Border Attribution

In some instances, it may be appropriate to look beyond the individual perpetrator(s) to determine what nation held the responsibility for the action. To assign state responsibility for a cyber operation that impacts national security at the international level is an arduous process legally and politically.

2.9.3 Cross Border activities:

When a business merges or buys another, a variety of legal and financial repercussions may be anticipated. According to clause 234(1)(a), an amalgamation occurs when two or more businesses incorporated in India or earlier under the businesses Act 2013 join with another company registered in one of the foreign countries named in section 234. According to Section 230 of the Companies Act of 2013, a merger is an arrangement in which several classes of shares are consolidated and then divided into separate classes. Accordingly, a cross-border merger would be regarded as an arrangement. The “Reserve Bank of India (RBI)” has published proposed regulations for cross-border mergers that address foreign exchange control. Cross-border mergers are now governed by the RBI (the "RBI Regulations"), which entered into effect on March 20, 2018. An agreement between an Indian firm and a foreign corporation is referred to as a "cross border merger" under the Companies Act of India. Section 234 of the firms Act only applies to mergers and amalgamations between Indian and foreign firms. However, the

Reserve Bank of India's regulations' use of the term "arrangements" may allow for agreements other than mergers and amalgamations. Mergers and reorganizations of Indian companies under the Companies Act are instances of this. [38].

2.9.3.1 Kinds and Classification of Border:

Two companies from two different economies combine their resources and activities to form a single legal entity through cross-border mergers and acquisitions. The target business is no longer an independent organisation. The transaction may be executed by an asset or stock exchange. The procedures needed to complete a merger transaction are often rather straightforward. In cross-border mergers, the shareholders of the target and takeover firms must be approved, and the acquiring company takes the goal's assets and liabilities. Two types of cross-border mergers exist:

- **Merger through Absorption:** It is the merging of two or more businesses into one already-existing business. Except for one, every company loses its unique identity. For instance, in the merger of HCL Technologies Ltd. and Intel Cent India Ltd., the latter completely lost its identity, while the former maintained its identity following the transaction and HCL acquired all of Intel Cent's assets and liabilities, allowing HCL Technologies to maintain its identity after the merger.
- **Merger through Consolidation:** In this form of merger, all the companies involved in the deal lose their existence and an entirely new company is created. The recent deal between Centurion Bank and Bank of Punjab leading to the creation of Centurion Bank of Punjab is an example of merger through consolidation. One essential feature of a merger either in the form of absorption or consolidation.

The two types of cross-border acquisitions: “Asset acquisitions and Equity acquisitions”.

- When a buyer buys a target's assets, this is referred to as an asset acquisition. It is, nevertheless, possible to recoup money from a significant asset sale by liquidating the deal's goal.

- Buyers that are buying a privately held company have the option of negotiating directly with the shareholders. The deal is handled by the acquirer and its parent to buy a fully owned subsidiary of another company. A large number of disorganized shareholders may be required to be bargained with by the acquisition firm when the target's shares are publicly held. This is when a public tender offer for the company's remaining shares is typically made. One benefit of share purchases is that they are easy to conduct and can be carried easily.

2.10 National Security Dimension of Cybercrime

Definition of national security. According to the Macmillan Dictionary, the general security of a country and a nation state is a common dictionary term. In a similar vein, “A country's national security is its ability to protect itself from the threat of violence or attack”, according to Collins Dictionary. "Nation" and "Security" are two key elements that make up "National Security." The "nation" is relatively recent and is merely a synonym for "nation state." The 1684 Treaty of Westphalia, which acknowledges nations' ability to self-govern their territory free from outside intervention, is when the term "nation state" first appeared. This phrase was further supported by the French Revolution, since France is frequently mentioned as the first nation-state following the French Revolution. The concept of "security" originated when prehistoric people recognised dread in the early stages of survival, and it still has the same meaning now. "Untroubled by danger and fear" is the definition of security. The most basic human need has always been security, and it will continue to be so in the future. Therefore, national security, which has traditionally been linked to military security, is simply the security of a nation state. But as events have changed, so too has the definition of "national security." Numerous political scientists and philosophers have provided a range of definitions. These definitions include simpler ones that focus on protecting the country's territory from political pressure and military attacks, while more complex ones add non-military aspects like “economic security, terrorism prevention, crime reduction, energy security, environmental security, food security, and cyber security”, depending on the situation at hand.

2.10.1 Changing Dimensions of National security:

Realism has been linked to national security, which gained significance during the Cold War in particular. The majority of countries declared their national security in terms of military security since the Cold War had such a profound effect on national security. The globe was split into two military blocs during the Cold War, and national security was determined by a country's

military might. However, there was a noticeable change in the definition of national security after the end of the Cold War [39].

2.10.2 Definitions of National Security:

The some listed widely accepted definitions of national security since its inception that demonstrate how the idea has expanded to encompass nonmilitary issues.

- A nation has security when it does not have to sacrifice its legitimate interests to avoid war and is able to, if challenged, maintain them by war," said Walter Lippman in 1943.
- Security, in an objective sense, measures the absence of threats to acquired values, and in a subjective sense, the absence of fear that such values will be attacked," said Arnold Wolfers in 1962.
- According to Harold Brown, the US Secretary of Defence from 1977 to 1981, "National security is the ability to preserve the nation's physical integrity and territory; to maintain its economic relations with the rest of the world on reasonable terms; to preserve its nature, institutions, and governance from disruption from outside: and to control its borders.
- The National Defence College of India seminar proceedings from 1996 state that "National Security is an appropriate and aggressive blend of political resilience and maturity, human resources, economic structure and capacity, technological competence, industrial base and availability of resources, and finally the military might."
- The definitions provide a broad overview of the evolution of national security across time. The best method to comprehend national security now is to consider the necessity of maintaining the nation-state's existence via the use of military, economic, and political power in addition to diplomatic initiatives.
- According to Henry Kissinger, national security encompasses all of a society's efforts to endure or accomplish its goals on a global scale.

- National security, according to Stanley Hoffman, is defending a country against external threats and shielding its economy from blows.
- According to the Atlantic Charter, national security includes both the freedom from fear and the goals that the people of a country have for their business and way of life.
- Richard Ullman makes the case that social discontent, economic instability, and resource scarcity should all be included in national security because he believes that non-traditional threats have the same potential to destabilise states as traditional military threats.

The efforts made by nation states to protect their identity, survival, and interests while taking into account present and future global changes and advancements are referred to as national security, according to international relations specialist Amin Hemedy.

According to Water Lippman, a country is genuinely safe when it can defend itself militarily if needed and preserve its rightful interests without sacrificing them to advert confrontation.

- The Five characteristics of National Security as follows:
- The state existence as a political community and nation
- Territorial integrity must be safeguarded and upheld by the state.
- To preserve the internationally recognised state's political autonomy.
- Assuring a state's quality of life
- Ensuring that the national security policy protects the state's fundamental interests

According to the researcher, maintaining society norms, laws, institutions, and values as well as the state's structures, values, and institutions are all part of national security. It also includes protecting people from both military and non-military threats and preserving their basic needs and liberties. We observe that the notion of national security has evolved from merely international borders and barriers to fault lines. The evolving nature of global threats and the increasing interdependence of states in tackling global security concerns are reflected

in this evolution. Sovereignty is essential to security, and the former cannot be achieved without the latter. National security and the tenets of international law interact on a global scale, influencing how states act. A framework for resolving international disputes and creating standards to advance security and peace is provided by international law. The United Nations Charter will be recognized as the primary body of international law/guidelines covering national security, when adopted in 1945. It identifies maintaining worldwide peace and security as its primary responsibility and expressly prohibits use of force in international relations, except in instances of self-defense. This prohibition also serves to reinforce the concept of sovereign equality among states and demonstrates the United Nations preference for communication and diplomacy rather than military force as a tool to contain hostilities and maintain international peace.

International law guarantees a state's right to self-defense, as this right is an inherent attribute of national security. Additionally, states are afforded the right to use force to repel assaults against themselves. In order to define the limits of state ,the principles of necessity and proportionality are applied, thereby ensuring responses to armed attacks are proportionate and reasonable. Furthermore, these principles create a requirement to lessen civilian casualties, protect civilians and respect human rights while at war. It also addresses the social and economic objectives that society wishes to pursue. British rules passed by the British Parliament in 1789 served as the model for India's national security laws. The Indian Council Act of 1861 was the first piece of law. 28. The Act gave the Governor-General the authority to periodically issue directives that would be necessary for the preservation of security, peace, and effective governance of the territories of any portion of them. The Act's terms "peace," "security," and "good governance" have served as the foundation for contemporary security legislation around the world.

2.10.3 Relationship between cybercrime, privacy, and security:

The “relationship between cybercriminal activity, privacy, and security in today’s digital environment” (i.e., “cyberspace”) is profound; deficiencies in security will always compromise both the privacy of users and organizations and be exploited by cybercriminals. Cybercriminals use weaknesses within digital security systems to illegally access computers, networks and/or data without consent. As a result of insufficient or defective digital security systems, cybercriminals can steal data, assume other people's identities, conduct illegal surveillance, and commit financial fraud all activities that violate an individual’s or organization’s right to privacy.

Cybercriminals can view privacy as both an objective and a byproduct of cybercrimes. Cybercriminals target personal data, sensitive communications, and digital identity as the most important types of assets. Cybercriminals use methods such as large-scale data breaches, phishing attacks, ransomware, and spoofed emails to expose, modify, and profit from the private information of individuals. Therefore, violations of an individual's privacy can be seen as tangible evidence of successful cybercrime activity.

Through the protection of users against cybercrime and from privacy violations, Security acts as a bridge between both. Cybersecurity poses an effective means of reducing the likelihood of Cybercrime and safeguarding the user's privacy rights via Encryption, Access Control, Authentication Mechanisms, Legal enforcement. But a lack of proper protection only increases the chances of cybercrime occurring, and further diminishes the Trust Users have with respect to Digital Systems, Government, and Emerging Technologies.

Policymakers must ensure that a focus on security does not outweigh the need for privacy protections or there may be an increase in the scope and extent of surveillance and misuse of personal information. Table 2.4 presents, relationship between cybercrime, privacy and security. Additionally, privacy frameworks without proper security measures are ineffective. A comprehensive Privacy Centric Security Approach, which aims to both protect individuals from

cybercrime and promote Data Protection Principles, Individual Autonomy, and Human Rights, is essential in achieving this balance[40].

Table 2. 4 Relationship between cybercrime, Privacy and security

Aspect	Cybercrime	Privacy	Security
Meaning	By using Digital system, the illegal activities are conducted	Protection of Personal and sensitive data	Safeguards protecting systems, networks and data
Major role	Acts as a Threat	illustrates a basic right	Acts as a Defense Mechanism
Main objective	Fraud, Data Theft and disruption	jurisdiction over personal data	Prevention, detection, and response to attacks
Interconnection	exploits benefit of security holes	Cybercrime violates	safeguards privacy and stops cybercrime
Targets	Users, networks, and systems	Digital identity and personal information	Users, data, and infrastructure

Effects of Inadequate Security	Increases the number of cybercrime occurrences	It causes privacy violations	leads to a compromise of the system
Data Participation	Misuses data that has been stolen or altered	Emphasises the ethical and legal usage of data	Ensures secure data handling
Legal Dimension	Criminalized under cyber laws	Protected by data protection laws	Mandated through cybersecurity regulations
Risk Factor	Causes financial and reputational loss	Causes identity theft and surveillance risks	Reduces overall digital risk
Technological Dependency	Uses advanced tools and techniques	Depends on secure data processing	Uses encryption, firewalls, and monitoring
Trust Implications	Erodes public trust	Builds trust when respected	Restores trust when effective

Policy Focus	Deterrence and punishment	Rights, consent, and data minimization	Prevention, resilience, and compliance

Surveillance Concerns	May exploit surveillance tools	Can be threatened by excessive monitoring	Must balance security and privacy
Human Rights Aspect	Violates individual rights	Upholds dignity and autonomy	Must align with human rights standards
Strategic Balance	Needs strong countermeasures	Requires protection-oriented policies	Must be privacy-centered and proportionate

2.11 Cyber risk management and cyber-resilience:

Malicious external attackers frequently use cyber threats (such as virus attacks, denial-of-service (DoS) attacks, financial fraud, system penetration, and proprietary information theft), whereas malicious internal attackers use illegal access to compromise the integrity, confidentiality and accessibility of data belonging to individuals, companies, and nations. This has an opportunity cost for businesses in addition to negatively impacting market capitalization and brand value. IT security (such as perimeter and core security systems) accounts for a large percentage of the “information technology” (IT) expenditures made by organizations and governments.

Because of the information era's rapid progress and reliance on Internet usage worldwide, particularly in India, cybercrime poses a threat to society. Cybercrime is not limited by geographical boundaries since it occurs in an international, borderless environment. India is a sitting duck in this situation since local laws are powerless to stop these atrocities. India has signed bilateral agreements, including a framework agreement with the United States and a cyber accord with Russia, to fight cybercrime[41].

These bilateral agreements are insufficient, ineffectual, and have a narrow reach when it comes to fighting cybercrime. India needs a multilateral treaty that will address international collaboration in fighting cybercrime globally and harmonize its laws through a single criminal policy. The pact should support the creation of strong investigative methods and efficient laws that can promote global collaboration in the fight against cybercrime. One such international multilateral agreement that addresses global collaboration in the fight against cybercrime is the Council of Europe's Budapest Convention on Cybercrime. Like the United States and Israel, with whom India has bilateral agreements to combat cybercrime, India need to sign the convention.

Cyber Resilience was selected as the data source because of its extensive subject coverage, wide range of journals. To determine inclusion and exclusion.

- **Cybersecurity Risk Management Processes (CRM's):** As a way to provide a clear plan, steps and procedures to identify, guard against, detect, react and recover to Cybersecurity Attacks. Organizations need to have a complete Cybersecurity Strategy that should outline the organization’s Cybersecurity Targets, Goals and Actions to achieve Cybersecurity Resiliency for the organization throughout the business life cycle. Cybersecurity Strategy includes outlining Cybersecurity Targets, Goals and Actions to successfully achieve Cybersecurity Resiliency for the organization throughout the Business Life Cycle.
- **Employee Information & Training:** Many organizations overlook the Human Element of Cyber security. Human elements represent the weak link in many Cybersecurity risk mitigation processes and, therefore, organizations are required to prepare and educate their employees and make them aware of Cybersecurity
- **Cybersecurity Visibility:** Organizations need an extensive level of visibility in their IT environment to identify Cybersecurity Threats quickly and effectively react to the Threats promptly

- **Cybersecurity Communication:** There need to be effective communication channels to enable organizations to quickly convey information about Cybersecurity Threats and Cybersecurity Attack Incidents.
- **Cybersecurity Continual Improvements**: Organizations should continually improve their Cybersecurity Posture to be proactive in the detection and remediation of Cybersecurity Threats by routinely evaluating their Existing Cybersecurity Controls and Processes.

2.12 Cyber Resilience:

In today's world, there are numerous types of "cyber threats, including malware, ransomware, phishing, DDoS attacks", etc.; not only do these threats lead to potential financial loss, but they also destroy the trust that consumers had in businesses, and the operational integrity of businesses is undermined by cyber-attacks. Over time, the concept of "Cyber Resilience" has become increasingly significant, in relation to business continuity, and provides a mechanism to ensure that organizations are able to operate securely whilst facing cyber incidents, and be able to react and recover from a cyber incident with relative speed.

The issue of Cyber Security and Privacy issues of SMEs in Canada, the research identified the most relevant issues from both Internal & External stake holders' perspectives; therefore, to address these cyber security/privacy issues, it is necessary to develop customized solutions/plans which will require strong "collaboration and a Multi-Stakeholder Approach" to maintain the delicate balance between internal obligations and the growing body of international regulatory requirements. Fig 2.14 represents Cyber resilience.

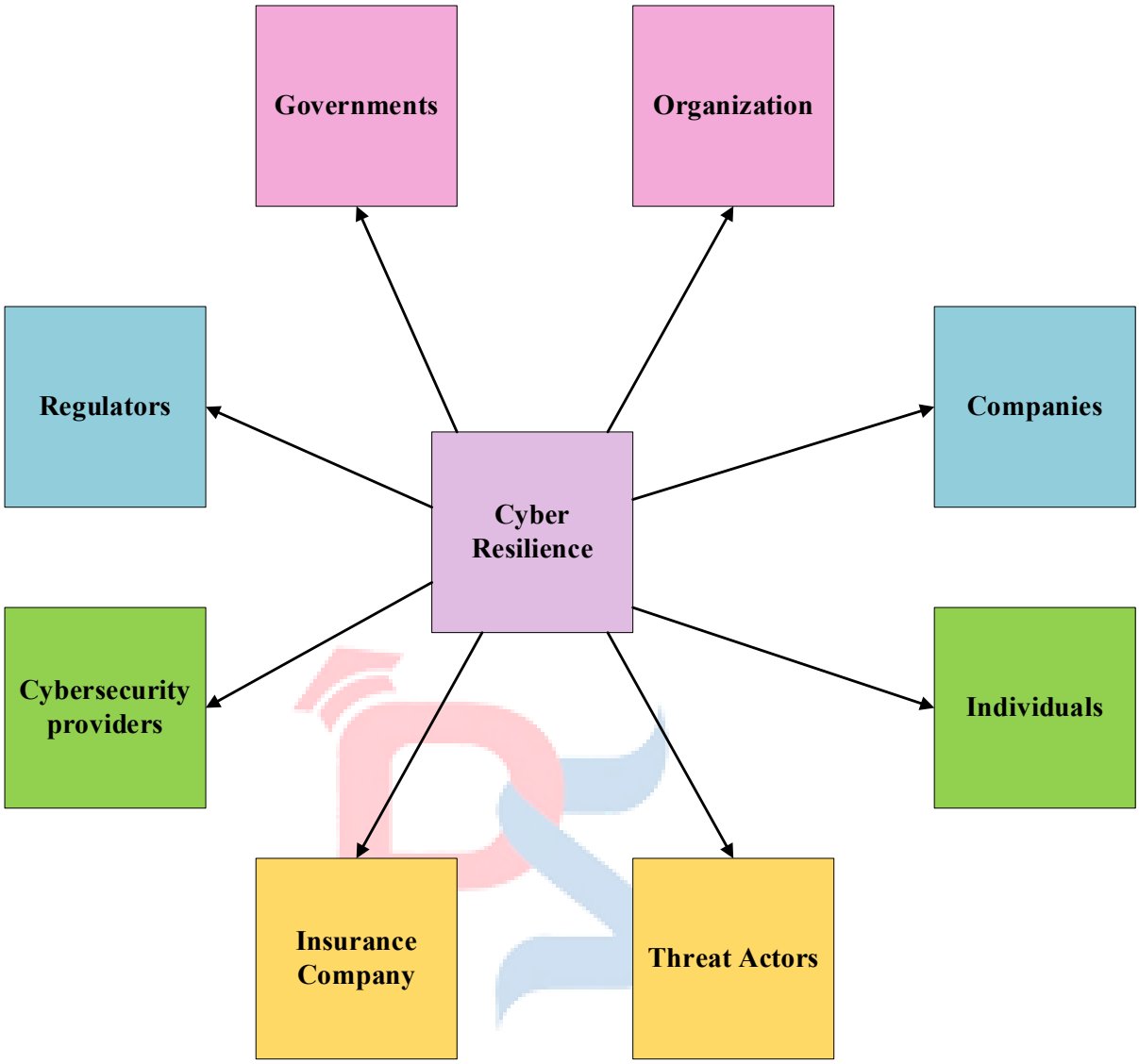

Fig 2. 14 Cyber Resilience

AI For Enhancing Cyber Resilience:

The rise of AI in cybersecurity, revolutionizing the way we think about the future of cyber resiliency. The use of AI within digital marketing has created dramatic improvements in the overall security framework of these initiatives by allowing organizations to quickly identify and respond to cyber threats. Organizations can now proactively manage current risks and anticipate potential "future vulnerabilities", thanks to this emerging technology. One of the key advantages of artificial intelligence is its ability to process large volumes of user behaviour data and network activity, allowing businesses to identify potential risks to their operations in real-time, thereby preventing disruptions from occurring prior to the opportunity of worsening.

However, despite these many benefits offered by this technology, there are also limitations including potential for fraud due to loopholes within the algorithm, and the challenges presented by limited internet access which may create distrust among some customers. There has been much discussion in the academic community about the duality of AI in strengthening both the weaknesses and strengths of digital marketing systems. While there is extensive documentation regarding the capabilities of the technology to provide enhanced cyber resilience through analysis of vast quantities of data, much research discusses the challenges surrounding AI, including the possibility of fraud, and security vulnerabilities.

The literature in publication has examined the “integration of AI into digital marketing systems”, emphasizing the necessity of implementing AI within a sustainable cybersecurity framework to improve “long-term resilience”. Furthermore, the In order to safeguard data and customer confidence, research highlights the significance of tackling current risks while making sure that security solutions are flexible and long-lasting [42].

2.13 IoT vulnerabilities and attacks:

The Internet of Things is rife with vulnerabilities. A taxonomy of IoT vulnerabilities. The IoT Devices Vulnerability statistics for Palo Alto Networks display the weight of different types of vulnerabilities. The user is the weakest link in the security ecosystem. IoT security issues are caused by a variety of sources. In the realm of Internet of Things (IoT) devices, security is becoming increasingly critical in modern times due to the proliferation of these devices. Therefore, having a systematic and well-established methodology for identifying and analysing IoT vulnerabilities is essential to ensuring protection from potential attacks and vulnerabilities associated with IoT devices. Each phase of the methodology provides a better understanding of the security posture of an IoT Device, so that organisations can improve their defences against emerging threats and vulnerabilities. The following phases detail the required knowledge and methodologies for thoroughly investigating and assessing IoT vulnerabilities, ultimately contributing to a more secure and safer IoT ecosystem, regardless of whether you are an organization looking to secure their IoT deployments or a security professional or developer.

2.13.1 IoT Vulnerabilities Layer:

Adversaries may gain access to this in a number of methods, including through software, hardware, or network flaws. The other “part of the attack layer” represents how these vulnerabilities are exploited. Any IoT device can be easily attacked by an adversary using any of the vulnerabilities, and they can choose to target availability, “data integrity, confidentiality, or authentication”. In order to prevent unauthorized access to IoT devices and data, confidentiality is typically enforced through the use of encryption, access control, and user and data authentication. By implementing encryptions, input validations, interface monitoring and limits, and many other measures, integrity usually ensures the protection of unauthorized modifications to a device's hardware or software. These are made to prevent vulnerabilities in any part of the device. Once more, though, tiny details. Fig 2.15 presents Iot vulnerability.

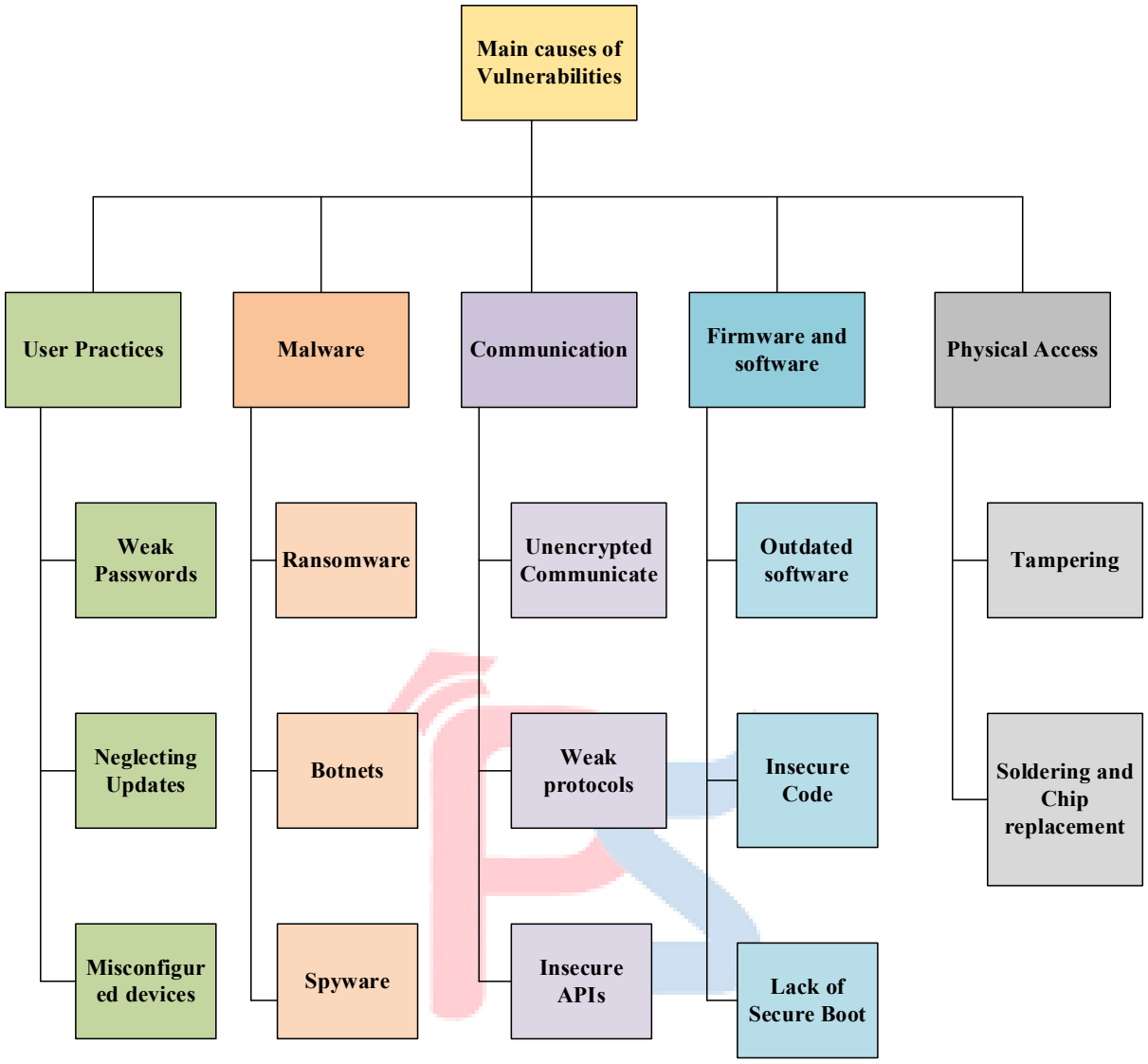

Fig 2. 15 IoT Vulnerability

are usually missed during the design stage of a device, which would enable the attacker to utilize it for their own nefarious ends. Accountability is the concept of monitoring activities and tasks to ensure that the gadget is performing as intended. In other words, it keeps an eye on everything the gadget does and restricts it to certain tasks. An attacker might get access to a device and alter the event path due to manufacturer weaknesses. This enables them to change how the devices operate or even send data to them for data monitoring. The last idea is availability. The device's continuous accessible when the user needs it is referred to as availability. An attacker can weaken availability by delaying or even taking the device

down when they target certain vulnerabilities. The kinds of assaults that an adversary can launch are the cause of all these security effects. if the attack is network, software, or physical

2.13.2 Network Vulnerabilities:

Two distinct subsets of networks can be distinguished from the concept of a network. WiFi and Ethernet are the common networks that are discussedBecause this type of network has direct connection to the Internet, devices may connect to it. Another type of network that is not often considered is the network of other wireless communications. This might be a Bluetooth, Zigbee, UWB, or many other types of networks. This network is called a wireless sensor network because it often comprises of several wireless sensors using different wireless protocols [43].

2.14 Cyber threat Intelligence:

"Cyber Threat Intelligence (CTI)" is a technology that helps improve information security. CTI provides information on defences and threats. If the necessary CTI is located, businesses may benefit from protective knowledge. However, corporate organisations have a variety of business process dynamics that could change the parameters at any time. Threats associated with contextual risk variables may also fluctuate over time.

Businesses may find that CTI-based defence strategies lose their effectiveness as conditions change. However, the existing methods for connecting the CTI to the business risk context are quite limited. The recommended model is a dynamic CTI model based on business processes (Singh & Mannepalli 2021). The dynamics of business environments can be seen and recorded by the model. To demonstrate how the model is used and how it modifies the connection methods in response to dynamics, a case study has been conducted. Software as a Service (SaaS) has gained rapid acceptance enabling applications and services to operate on software cloud platforms. Despite SaaS's widespread use in cloud computing, the security challenges that web apps utilising cloud SaaS must address cannot be concealed. Cloud apps are vulnerable to the majority of popular web assaults, much like other online-based systems. SQL injection is one of the biggest threats to a SaaS application. This may lead to the loss of sensitive and important data (personal, financial, etc.). Sensitive information can be stolen from a business or organisation by an attacker, causing significant harm to both intangible (like reputation) and tangible (like data) assets. The goal of this research is to ascertain whether it is feasible to detect SQL injection at the application level using machine learning techniques. The algorithms that will be tested are classifiers that have been trained on a range of hazardous and benign payloads. After a payload is received as input, it is analysed to determine whether any dangerous code is present. The results demonstrate that these algorithms can differentiate between malicious and genuine payloads and have a detection rate of over 98%. Additionally, the study evaluates the effectiveness of several machine learning algorithms in identifying SQL injection risks. From

the perspective of a cloud user, there is no guarantee that the co-resident virtual machines can be trusted. Co-resident invasions, in which one coresident virtual machine invades another, are made possible by shared resources, which provide unthinkable privacy and perfect separations. Fig 2.16 represents cyber threat process. We talked about the security solution based on an augmented relevance vector machine with fuzzy c-means clustering (IRVM-FCM), which lessens Co-location DOS intrusions by making it harder for attackers to launch an attack.

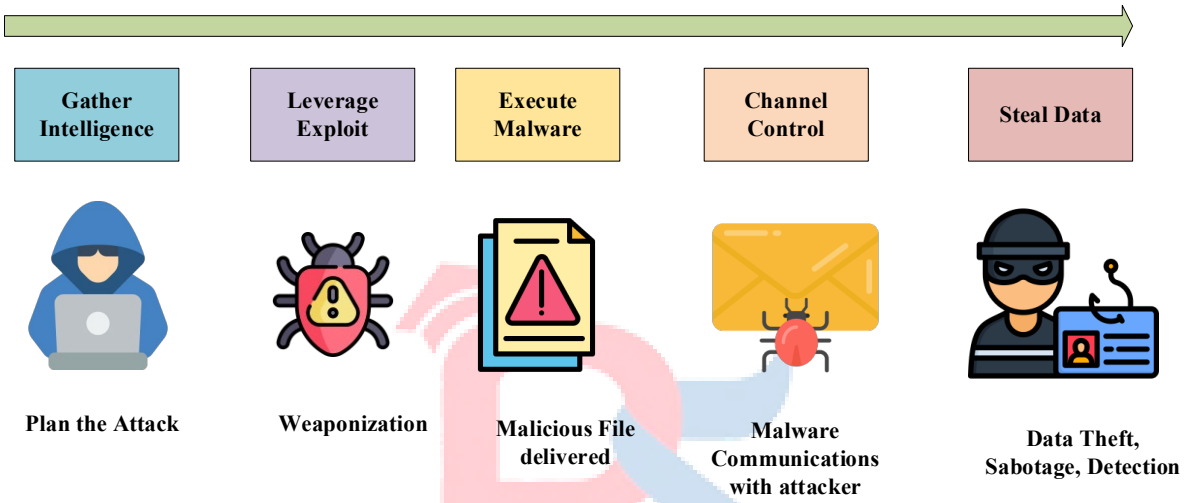

Fig 2. 16 Cyber Threat Process

Emerging Threat and Challenges:

The "cyber threat landscape" is rapidly evolving due to advances in technologies such as "blockchain, artificial intelligence, and the Internet of Things". While these advancements create many opportunities for organizations to take advantage of, they also introduce new vulnerabilities that cybercriminals are risking more frequently on a daily basis. Cyber threat intelligence provides organizations with a fighting chance against the new breeds of cybercriminals, who are continuously developing more creative ways to bypass existing cybersecurity systems and find previously unknown vulnerabilities. The emergence of "Crime as a Service (CaaS)" in the web is elevating the threat level associated with CaaS, forcing companies to collaborate on strategies to gain an understanding of the evolving CaaS threat landscape and create the ability to combat its effects. In addition, the dark web offers a wide variety of opportunities for hackers to engage in the vulnerability exchange process, thus

allowing them to be better informed about the attitudes and tactics of other hackers and leveraging this knowledge into a more successful cyber attack. Through their classification methods for forum content, the authors reveal the early stages of hackers' preparations so that organizations can predict their future actions. This alters how organizations view Cyber Threat Intelligence (CTI); previously CTI was thought of primarily as a means to protect against attackers reactively, whereas now it is viewed as a strategic advantage. The authors emphasize that there are significant risks associated with sharing CTI, particularly when an attacker has access to sensitive information such as code vulnerabilities or the ways that a company operates internally. The study points out that trust between the entities sharing CTI is critical for success and provides a means of conducting risk assessments to quantify the risk of either party being exposed to each other's sensitive data, and the potential consequences of such exposure. The study also outlines some of the barriers to effective sharing of CTI, such as a lack of trust, fear of privacy violations, and the need for organizations to comply with the General Data Protection Regulation (GDPR) even though sharing of CTI is vital for enhancing defense against cyber-attacks. Anonymization and removal of excessive data is encouraged to mitigate these risks and facilitate the safe exchange of CTI between organizations. The authors examined the pros and cons of popular frameworks and methodologies for mapping attackers' Tactics, Techniques and Procedures (TTPs), including “Data Flow Diagrams (DFDs)”, “STRIDE”, “Attack Trees”, and frameworks such as “MITRE ATT&CK and the Cyber Kill” Chain. This study concluded that many of the examined models were missing automated capabilities, thus supporting the idea of merging predictive analysis with machine learning to improve the detection and remediation of APTs and the effectiveness of the organisation's overall threat response against high-risk threats. The report underscored that the emergence of new technologies such as (AI) and (IoT) technologies has greatly expanded the size and scope of the threat landscape. The study examined defensive measures that leverage machine learning-based detection algorithms, demonstrating their ability to detect evasive and low volume attacks. To enhance the resilience of the financial sector, the study also emphasised the need for collaboration between banks, the private sector and government entities and

highlighted the importance of developing security regulations and educating employees on cybersecurity to decrease human error.

Organizations are being transformed by machine learning and automation in managing large amounts of data allowing for quicker and more effective threat detection. To enable organizations to effectively share and use threat intelligence, the authors of this study proposed using standardized formats such as TAXII and STIX to create interoperability between shared threat intelligence systems.

In addition, the study has recognized that the use of social engineering techniques, as well as new types of zero-day attacks, require organizations to adopt more proactive and adaptable approaches to detection. By improving their capabilities for detecting cyber threats, organizations can enhance their resilience against rapidly developing, emerging threats, while moving from the traditional paradigm of reacting to threats to employing proactive approaches.

Cyber Threat Intelligence Lifecycle:

The CTI life cycle is a systematic, continuous procedure that produces TI. Data and information about dangers are found and gathered during this procedure in order to produce CTI.

Stage1: Planning and Direction

Planning and Direction: The most crucial phase of the CTI lifecycle is planning and direction. The CTI users, intelligence needs, and intelligence priorities are determined at this point. At this point, there is a significant amount of cooperation between CTI producers and consumers. The intelligence collecting plan, which includes the scope and purpose of intelligence, is frequently outlined in the planning and directing phase output.

Stage2: Collection

In this step, a variety of sources are used to collect the desired intelligence data that was outlined in stage one. For analysis and exploitation in the next phase, organisations actively

gather a variety of threat categories, such as phishing attempts, compromised credentials, vulnerabilities, and network logs. The organization's specialised security teams are frequently in charge of collecting logs. Numerous data kinds, including network, system, application, and security event logs, may be included in these logs.

Stage 3: Processing and Exploitation

The data collected the previous stage is processed for use in this stage. Threat data is gathered in step 2 as raw data, and during the processing step, it is normalised, organised, structured, and transformed into information that can be used immediately in Stage 4. Data processing operations including “structure, data correlation, parsing, and data reduction” may be applied at this step (step 3) using automated tools.

Stage 4: Analysis and Production

This level involves analysing, integrating, interpreting, evaluating, and translating the processed intelligence from the previous stage into contextual knowledge and meaningful intelligence, such as threat actors, events, and attributes. To give both qualitative and quantitative evaluations, further data analysis tools, such as statistical approaches and machine learning-based techniques, may be used at this point. Following an analysis of the threat intelligence, the threat intelligence's importance, severity, and consequences based on the evaluation of the company and environmental context, which aids in the creation of a qualitive[44].

Stage 5: Dissemination

This step reports the intelligence that results from the Analysis and Production Stage (Stage 4), taking into account the confidentiality and intelligence priority established during the analysis stage. Translation of the threat intelligence is necessary for the dissemination step. Fig 2.18 represents Lifecycle of Cyberthreat Intelligence.

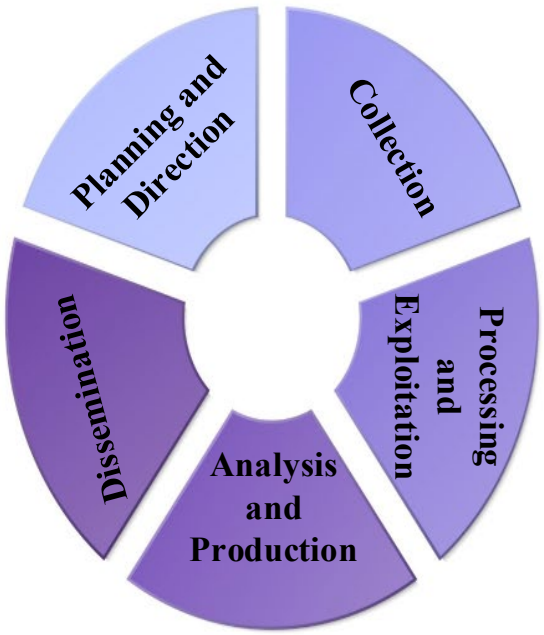

Fig 2. 17 Lifecycle of Cyber Threat Intelligence

Cyber Threat Intelligence uses are:

The following procedures are some of the most typical ways that CTI is used in the organizations mentioned in the aforementioned studies:

- Improving detection capabilities
- Blocking threats
- Security awareness
- Threat management (for identified threats)
- Vulnerability management
- At-risk asset identification
- Incident response
- Threat hunting

- Risk management
- Prioritizing security controls
- Vulnerability remediation prioritization
- Cyber threat modeling
- IT operations (troubleshooting infrastructure)
- Security awareness training for staff
- Security standards compliance
- Decision making for security budgets

CHAPTER 3

REVIEW OF LITERATURE

In this chapter, you will find a description of the main efforts of several governments in fighting different types of internet crime and the current cybercrime. The chapter evaluates how effective the various tools available within the legal framework have proven to be in dealing with the growing threat posed by cybercriminals and seeks to determine what the key challenges for enforcement and compliance are when it comes to this area of law.

3.1 Cybercrime and National Security Threats:

The author thoroughly examines cybercrime in “Small and medium-sized enterprises (SMEs)” using “cyberspace theory”. Cyberspace theory, which looks at the causes, effects, and gaps of cyber events, makes it possible to properly evaluate cybercrime in SMEs. Using information of a sizable “European Union database” that comprises SMEs from member countries, our work is created and based on SMEs' “perceptions of cybercrime”. Improving cybersecurity procedures and recognizing “broader economic and societal repercussions of cybercrime” require an understanding of SMEs' perspectives on cybercrime [45]. The “Federal Bureau of Investigation” and the “National White Collar Crime Centre” provided data used in this article, which looked at the trends of cybercrime victims from 2001 to 2021. It looked at patterns in cybercrime victimization, with a focus on Australia, in order to draw conclusions regarding Papua New Guinea (PNG). The results confirmed that the number of Internet users who became victims of fraud increased dramatically between 2016 and 2021.

According to World Bank data on Internet use, the number of Internet users in Australia and PNG will increase at a minimum rate of 1% to 2% over the next few years. The conclusion is that

Cybercrime will keep increasing unless PNG establishes strong cybersecurity regulations and institutional capacity [46]. The paper offers studies that show a relationship between perceived vulnerability and the usage of computers and other electronic devices, as well as a comparison of how people in rural and metropolitan areas perceive cyber victimisation. Our field study yielded a representative sample of the European Republic of Slovenia. Urban dwellers were more likely to report some cybercrimes, such as hate speech, rumors, and indecent content. Future research should concentrate on how people understand topics that are commonly used and studied in cybersecurity research, such as ransomware, phishing, and wireless network interference[47].

According to the author, cybercrime has societal effects as well. People who are victims of cybercrime often worry, feel anxious, and fear becoming victims again. Communities suffer from social division and a lack of trust. The authors suggested a method for assessing the socioeconomic impacts of cybercrime and oversaw research into these effects. If law enforcement and policymakers have a more precise understanding of cybercrime, they will be better equipped to prioritise the battle against it [48]. Cybercrime in SMEs may be accurately assessed thanks to cyberspace theory, which examines the causes, consequences, and gaps of cyber occurrences. Our work makes a contribution by developing a “taxonomy based on SMEs'” insights of cybercrime anxiety using data via a large “European Union database” that contains “12,863 SMEs” from “member nations”. Accepting SMEs perspectives on cybercrime is essential to improving cybersecurity practices and recognising the wider cost-effective and societal repercussions of cybercrime [49].

The study article employs semi-structured interviews, a qualitative research method, to identify the major factors influencing cyberattacks in developing nations. Experts in cybersecurity employed in Pakistan's financial industry provided the information. According to

the report, the primary causes of the lower financial losses are the opportunity cost of cyberattacks and the smaller attack surface in poor nations like Pakistan. The study's conclusions will promote the use of cutting-edge cybersecurity technology in emerging nations' banking and finance sectors, such as AI and ML [50]. The author illustrates a new category of criminal activity occurring in the metaverse that poses a danger to both conventional digital criminality and the current legal systems. the parallels and discrepancies between conventional cybercrime and meta crime using a multidisciplinary literature review and comparative analysis. These two types of crimes were shown to share five characteristics: anonymity, ongoing evolution, criminal classification, hyper-spatial-temporality (global reach), and governance concerns. The results showed that an absence of consciousness and trust in the authorized. organization led to insufficient reporting of cybercrime incidents [51]. The author presents factors influencing cybercrime victimization are presented throughout the essay, and "Routine Activity Theory" (RAT) is regularly provided . However, its conclusions regarding RAT theory's applicability are not totally consistent. This will reduce some of the "inaccurate measurement issues" with the "RATS" structures that have led to inconsistent findings regarding the victimization of cybercrime. Security advocates could use the study's findings to develop relevant cybercrime programmed for awareness. The online traits, activities, and strategies for combating cybercrime [63].

The article present state of the literature on the use of a human-centric investigative method (i.e., profiling) to cybercrime, this systematic review set out to conduct a qualitative meta-synthesis. The development of a comprehensive framework for employing profiling techniques to combat cybercrime is known as cyber behavioural analysis, or CBA. It provides the basis for knowledge in the field of cyber behavioural sciences, which aids in directing upcoming empirical research on the characteristics and behaviours of cybercriminals as well as the application of profiling techniques and procedures in cybercrime [66]. The article states that organizations in the UAE must improve their cybersecurity plans since cyber threats are always changing. The goal of these studies is to comprehend and combat both organized and unorganized cybercrimes in the United Arab Emirates. The proposed action steps are aimed at

lessening the likelihood of a data breach, improving overall organizational security planning, and encouraging stakeholder awareness of cybersecurity. By implementing this guidance, organizations can effectively enhance current system-level protections against cyberattacks and thereby decrease the probability and impact of cybersecurity incidents [67]. The paper presented by using the “Global Terrorism Database (GTD)”, the study retrieved and examined “high impact attacks (HIAs)” committed by radicals within India and its surrounding nations “since the 1970s”. Using the “iterative outlier analysis (IOA)” heuristic, we assessed the mining effectiveness of the “Global Terrorism Index Impact Score (GTI-IS)” in comparison to the “GTD measure”. These studies show that the statistical distributions of deadly and non-lethal attacks differ between various nations, which can help build targeted counterterrorism strategies [71].

3.2 Cyber Law and Institutional Enforcement

The research presented provides a tested and a uniquely tailored way to mitigate cybercrime in e-government services using a context-specific method through the use of the HOT Paradigm to aggregate the regional factors into a more effective method for reducing cybercrime in e-government services. This study offers helpful data for developing theoretical frameworks, enhancing operational procedures, and assisting legislators in developing successful cybercrime mitigation plans. It affects theory and policy as well [83]. The author is to offer insightful information about Vietnam's legal strategy for combating cybercrime. To critically evaluate how the legislation is applied in practice, it is also important to look at the history and training of LEAs, the attitudes of people and businesses regarding the current cybercrime law, and the development of cybercrime. In several aspects, it is constrained. Interviews were conducted with just seven senior cyber police officials who worked directly on cybercrime investigations [53].

According to the research paper, “Cyber Forensic Investigations (CFIs)” remains insufficient organization to deliver consistent information on the primary trends in cyberattacks. According to statistics from the “Global Cyber Security Index (GCI)”, Pakistan's serious organizational and technological shortcomings put the country's national security at danger. This essay concentrates on state-owned synchronized “CFI infrastructure” towards lessening the prevalence of cybercrime issues. To address the CFI infrastructure, a conceptual model that makes use of “organizational, legal, technical, policy, capacity-building, and cooperative venture techniques” was also created. Now, in the end, CFI is a critical phase for consolidating Pakistan's cyber security carriage and overcoming the problems with the existing cyber environment [54].

3.3 Privacy, Data Protection, and Legal Regulation

This article presents scholarly discussions about creating a new fundamental right related to cybersecurity under EU law but also discusses the relationship between a new right to cybersecurity and an already existing right to security. In addition, the article provides information on what will be included in the new right to cybersecurity, as well as possible methods of implementation. The conclusion of this article will argue for the acceptance of a new right to cybersecurity in EU law [55]. The research recommended National security is one of the main issues of the twenty-first century due to our growing reliance on technology. It increases the inherent risks of technology and poses several difficulties for both industrialized and developing nations in their efforts to combat cyberattacks. This research study evaluates GDPR-inspired legislation across the South Asian region in light of the much greater diversity that exists among Asian countries compared to European. The study's primary findings indicate that a number of South Asian countries are now reviewing their GDPR-compliant data protection laws [58].

The paper presents safe IoT is a modern necessity, and it is important to research vulnerabilities and assaults in IoT architecture. The scope and impact of cyber laws in several nations create challenges. For example, content on the internet may be legal in one jurisdiction but unlawful in another, making it challenging to create universal regulations [59]. The paper presents how the development of information accessibility poses numerous challenges to maintaining stable national security. Information technology can assist nations in identifying possible dangers, securely exchanging information, and implementing protective procedures in their national security strategies. The research primarily focusses on publicly accessible information, information that affects national security, cyberattack risks, and artificial intelligence (AI) as critical to national security for carrying information roles. As a result, information can be crucially implicated in sensitive information retrievals, the dissemination of misleading information, the creation of spam to mislead users, and potential privacy theft for

blackmail reasons. There are several examples of these limits of present functional domains [64].

The article presents artificial intelligence's explosive growth, which presents serious privacy and data security issues. The framework discusses data protection in AI, highlighting the significance of protecting the data used in AI models and outlining procedures and policies. Additionally, the security of AI is examined, including the risks and vulnerabilities in AI systems, examples of potential malicious manipulations and attacks, and security frameworks to lower these risks [73]. The purpose of this survey is to bridge the dearth of a thorough survey on the protocols used in FL systems and the numerous research on PPFL, where is adopted to provide a privacy guarantee. We examine the PPAgg techniques that have been suggested to handle security and privacy concerns in FL systems in this survey[38]. The hazards to people' privacy were categorized and explored based on the kinds of AI tactics employed by governments that could have a collective behaviour. The paper's conclusion discusses the creation of regulations based on the moral design of citizen data collection, with implications for governments looking to control security, ethics, and data privacy [81].

3.4 Emerging Technologies and Security–Privacy Balance

The primary goal of the paper is to demonstrate the use of XAI in Cyber Physical Systems (CPS), including the challenges, benefits and recommendations for implementing XAI in CPS. This research will focus on identifying the current status of XAI and CPS, exploring the various industries which leverage XAI for CPS, and recommending areas for future research. Within this paper, there are multiple innovative ideas for future research related to the development of multisensory explanations and outputs for CPS, utilizing XAI to improve employee well-being by reducing occupational burnout and enhancing employee engagement, and synthesizing the cross-disciplinary goals and benefits of XAI in Cyber Physical Systems [56].

The article presents technical implementations also attract adversaries and cybercriminals to commit crimes and launch assaults on these modern infrastructures. We offer a common infrastructure model for smart cities. To identify infrastructure threats and create a threat model that interested parties can alter or expand, we employ the Microsoft Threat Modelling Tool and the STRIDE threat modelling methodology in compliance with the criteria[61]. In this research study, we identify and analyses the primary barriers to the acceptance, promotion, and usage of blockchain technology that exist amongst SMEs, corporations, organizations, businesses, government agencies, and the general public. In order to initiate global conversations on health, finance, and market strategies that should incorporate all society levels, research in these areas is crucial. During experimentation, we identify the system needed for data detection, capture, processing, and storage. This involves isolating packet data to educate degrees of cybersecurity and privacy-related procedures, as well as making sure transparency is exhibited in a clever, secure, and effective manner [74].

The author presents to reduce present security and privacy issues, including data loss, data manipulation, and data theft, this project attempts to develop a data security paradigm for cloud computing based on cryptography and steganography. The four processes include data sharing,

data backup and recovery, steganography, and encryption mechanisms for data security and protection. By shielding data confidentiality, privacy, and integrity from hackers, this suggested method guarantees increased cloud data redundancy, flexibility, efficiency, and security [75].

This paper presents a revolutionary networked metaverse architecture and talks about its main features, enabling technologies, and current prototypes. In order to create customized security and privacy countermeasures for the metaverse, they examined current and potential solutions [76]. The study demonstrates FL has already been examined from a number of angles in previous surveys, but not enough progress has been made in comprehending FL's security and privacy threats. his gap by offering a thorough analysis of security and privacy concerns pertaining to federated learning. Lastly, the distributed architecture and classical machine learning present privacy and security challenges for the FL [77]. The paper presents IoDT's inherent features, including its "decentralized structure, information-centric routing, and semantic communications", which provide significant obstacles to the provision of security services. The IoDT is reviewed in this study in terms of system design, enabling technologies, and security/privacy concerns [78].

This study proposes the Triple Data Encryption Standard (TDES) technique to protect large amounts of data in cloud environments. An organization's capacity to adopt cloud services is restricted by growing worries about big data security and privacy. The existing approaches to privacy protection have several drawbacks, such as a "total dependence on third parties, inadequate data privacy and accurate data analysis, and inefficient performance". By utilising additional keys in DES, the introduction of the proposed TDES methodology creates a much easier method to prevent attacks and keep data private. The results from experiments conducted on TDES have demonstrated its effectiveness in preventing attacks on large volumes of data in cloud-based environments[79]. This Paper aims to provide a summary of existing literature on PPFL, as well as identify the absence of a complete survey regarding the implementation of PPAgg-based protocols within FL systems. In this survey, we look at the PPAgg approaches that have been proposed to address security and privacy issues in FL systems [80]. This study

focuses on developing an “Artificial Intelligence-based Lightweight Blockchain Security Model (AILBSM)”. Conventional IIoT architectures have challenges such as “centralization, loss of privacy, integrity, and trust” due to a number of security vulnerabilities and network intrusions. The integration of blockchain authentication and autoencoder-based transformation greatly improves the detection performance of the proposed method when compared to other approaches [82].

3.5 National Security Governance and Policy Dimensions

The article presents to develop an initial programmer theory, the research paper reports on expert stakeholder conversations and a scoping review. We searched electronic databases, webpages, and references for material that met the inclusion criteria. We looked at 52 main and secondary data sources to expand and enhance the programmer theory and create Context-Mechanism-Outcome Configurations (CMOCs) that explain how, why, and under what circumstances older persons become victims of financial cybercrime. After that, we extrapolated this data to think about sensible intervention techniques [52]. This research study demonstrated a new interdisciplinary method that focused on 'big data' cognitive computing through the incorporation of the 'personality theory', which has been shown through validation as well as other research, with a goal to combine the two fields in order to evaluate human behaviour through retrospective data analysis of large samples as opposed to the use of traditional measures such as surveys/interviews, which are considered less accurate and valid [84].

The paper presents of national security indices do not reflect any correlation between energy security and national security. Through regression modelling, only the USA indicates an observable correlation between energy and economic security; all other countries studied take no measurable association between energy, economic and security indices. Additionally, there are no existing long-term cross-national security indices that adequately measure all three aspects (i.e., economy, energy, and national security), making it impossible to create models that adequately capture all three factors [68]. The article presents national security indices worldwide and the literature search, researchers have often overlooked the interaction between energy security and national security. The only country that demonstrates a substantial impact of energy security on economic security, as evidenced by the calculated regression model, is the United States. In other countries examined, there appears to be little or no relationship between economic security and energy security, nor between either of these factors and national

security. Due to the absence of comprehensive long-term cross-country comparisons available to researchers, there is a scarcity of data reflecting actual cross-country comparability and therefore enabling predictive modelling of national security, economy and energy. The effects of national security-centric foreign investment screening laws upon globalization are explored through the meta-analysis of the business environment literature; further, the insights gained from this analysis will augment the findings within IB literature [69].

The article suggested Lithuania has developed tremendously since gaining independence and has risen to the top of the EU. However, it will be increasingly challenging to sustain this robust income growth in the future due to mounting fiscal pressures and an ageing and shrinking population. This essay looks at the primary financial problems and possible fixes. Immediate challenges like rising borrowing costs and military spending are outweighed by long-term pressures associated with population shifts and climate change. It produces outcomes like changes to tax rules meant to boost revenue while primarily focusing on reducing spending through modifications to the healthcare and pension systems [70]. The paper discusses how the selection of various functional components of transport tariffs affects their capacity to protect national security. Since the final criterion includes the traits of environmental footprints, economic growth, energy efficiency, and security, it was selected as a critical indicator of national security. The best design for transport taxes is chosen based on the study done to enhance its regulatory efficacy [72].

3.6 Summary:

The author presented indicates that concerns for national security caused by cybercrime have grown due to many factors, including the rapid speed of digitization and the reliance by people, “public and private sectors”, and government on information technology. Cybervictimization rates are higher among organisations than individuals, and, as a consequence of a number of other issues, these rates vary substantially over time. There also is considerable variation in the rates of cybercrime victimization among countries depending on their respective capabilities legally and/or institutionally. In general, weak cybersecurity law and ineffective enforcement of that law and the lack of sufficient cybercrime forensics capabilities are major obstacles to the effective control of cybercrime worldwide, particularly in developing countries. The emergence of AI, IoT, cloud computing, and cross-border data flows presents additional security, privacy, and data protection challenges. Emergent technologies' complexities with respect to the trade-offs between security and privacy that need to be solved through transparent, explainable, and ethical Because the financial loss and social and economic impact of cybercrime generate fear and mistrust toward individuals/organizations, these difficulties highlight the need for issues to be addressed by raising awareness through human-centric approaches. All of the above literature together has demonstrated that there must be a governance model that integrates technology, law, policy, and international collaboration for national cybersecurity.

CHAPTER 4

RESEARCH METHODOLOGY

4.1 Nature of Research:

4.1.1 Doctorial

The present research ("Challenges and Opportunities of Law in the Age of Digital Security") provides a methodology to demonstrate how a systematic approach to research allows a researcher to identify and analyze the legal aspects of the research, identify the relevant laws related to the area of research and to develop the appropriate framework and methodology for a comprehensive understanding of the issues associated with the various elements of the research related to Cybercrime, National Security and Privacy through Emerging Technologies. In this presentation of the methodology the research design is outlined and justified by the nature of the data and source of data, the comparative analysis and the methodology used to conduct the analysis of the Law associated with this research.

In the context of this research, doctrinal analysis is used to:

- Review the laws addressing Cyber Crimes, Security, Data Protection, Cyber-Surfing and Bio Security
- \Interpret the legislative intent of various laws that govern the use of Electronic Communications/Information Technology (i.e., the Information Technology Act (IT

- ACT), 2000, the General Data Protection Regulation (GDPR), and surveillance legislation).
- Analyze the basic principles of the Constitution including the Right to Privacy, Proportionality, and Reasonable Restrictions in relation to National Security.
- Study significant judicial opinions in cases regarding Privacy and Surveillance to determine how courts interpret the law as it relates to these areas over time.
- This approach is particularly well suited to the objectives of this research, which does not seek to produce new empirical data, but instead, seeks to evaluate how sufficient, consistent and coherent are the current legal regimes in existence. The conduct of doctrinal research will enable the researcher to identify any gaps, ambiguity or overlap within the law that impacts the competing interests between national security requirements and individuals' right to privacy.

4.1.2 Analytical

An analytical approach to research is used to assess how well current laws protect the public against new forms of digital crime while protecting people's fundamental rights. Doctrine-based research explores the law and its interpretation; however, by using an analytical approach to study how the law functions and is enforced, the researcher can determine if it achieves its intended purpose.

In this study, analytical research is applied to:

- Assess the efficacy of cyber law and surveillance methods for mitigating Cyber-terrorism, data theft (breaches) and Cybercrime (transnational, cross-border or otherwise).
- Determine how National Security laws affect the individual's rights, respectively Civil liberties and Personal Privacy.
- Assess any potential Conflict between Security Laws and Privacy Legislation.

- Identify the challenges of Emerging Technology i.e. Artificial Intelligence, Big Data Analytics and Mass Surveillance technologies.
- The Study's analytical evaluation identifies the structural weaknesses, enforcement challenges and ethical issues present within today's legal systems. The analytical evaluation is also an avenue for the research to move beyond merely explaining legal systems, and utilise a higher-level of critical reasoning to determine potential areas of legal reform and change in policy.

4.1.3 Comparative:

This study will use comparative legal research to examine how different jurisdictions deal with the relationship between national security and privacy issues related to digital technology. Through a comparative analysis, this research will demonstrate ways in which various jurisdictions have implemented innovative methodologies that can assist in shaping the best practices of enforcement and litigation, while providing examples of how the legal systems of different jurisdictions look at precedential cases and technology in relation to enforcement and litigation.

The following tasks will be completed by me during this comparative analysis process:

- Comparing India, the European Union, the United States, and the United Kingdom
- Analysing the regulations of each jurisdiction:
- Digital threats and Cybercrime
- Surveillance powers and Gathering of Intelligence
- Protection of data and privacy rights
- Mechanisms for judicial accountability and supervision.

Analysing differences in enforcement strategies, constitutional and statutory protection Investigate how various governance systems, laws, and policies have impacted the relationship

between security and privacy in relation to the growth and evolution of digital governance practices, as well as how this has happened globally, using the comparative method.This comparative method, by developing a framework of global norms for digital governance and identifying elements that may enhance or modify India's current legal framework, will allow you to identify possible ways to enhance or modify India's current governance practices.

4.2 Sources of Data:

This study uses a comparative analytical technique using the legal documents of the national government on the topic of privacy/security. The sources of the data to be analyzed include: the national constitution (usually by statute), laws of the national government (legislative acts), law books of the national government (statutory law), regulations of the national government (i.e., specific and detailed law), decisions of the national courts, and laws and regulations of foreign countries that pertain to Cybercrime, Surveillance Laws, and Data Protection Laws. Use of Academic Literature to Enhance Conceptual/Theoretical Analysis: In addition to the above sources, this study uses a holistic approach through the inclusion of Academic Literature including Textbooks, DOI-referenced Journals' Articles, Research Manuscripts, Doctoral Theses and Policy Reports to enhance its Conceptual/Theoretical analyses.

Other sources consulted include; reports of law commissions, reports prepared by Parliamentary Committees, Government Policy Documents, and international organization publications. These additional sources provide a view of how the above-mentioned sources meet various challenges and ways to reform the laws and regulatory frameworks governing Cybercrime. The study also provides comparative and International Materials AM, international legislation authored by Judicial Statutes. Such comparisons allow the comparison of laws in each jurisdiction although the legislative instruments may not have been enacted in each State/Jurisdiction. As many Laws regulating Cybercrime are Model provisions but not exact replicas of those Model provisions, the analysis ultimately gives credence to the concept of International Best Practice Guidelines. Authentic Information has been collected from reliable sources (i.e., Official Government Websites), along with Reputable Legal Databases to ensure that the data/Information collected and analyzed for this study are accurately sourced and cannot be mischaracterized, misapplied, or otherwise used for an unintended purpose.

4.3 Comparative Framework:

This comparative framework is intended to facilitate an analysis of how military conflicts and terrorism are addressed by the legal systems of several diff countries - specifically, India, the EU, the USA and the UK - and to develop a standard methodology for comparing laws, judicial interpretation/implementation of these laws, and the means of enforcing these laws so as to promote the development of "best practice" solutions to balancing security and privacy interests in the digital age.

4.3.1 Country selection

The study makes a comparison between India; the European Union (EU); the United States of America (USA); and the United Kingdom (UK) [85]. These jurisdictions were purposely chosen for the following reasons:

- India has an emerging digital economic landscape characterized by developing laws on cyber and privacy with both a growing judiciary and increasing powers of surveillance, provides a model of a transitional legal system.
- The EU has a rights-based and harmonized regulatory framework with the General Data Protection Regulation (GDPR) as an established global standard in terms of accountability for data protection, privacy and rights.
- The USA is using a fragmented approach to privacy and cyber regulations based on specific sectors, but focused primarily on National Security and National Law Enforcement capabilities.
- The United Kingdom has an extensive network of judicial accountability and compliance mechanisms; however, it takes a balanced view toward safeguarding an individual's privacy and protecting the country's interest in terms of security. A comprehensive understanding of hybrid regulatory/oversight systems within

jurisdictions is dependent upon understanding the post- GDPR (General Data Protection Regulation) regulatory framework.

- A relevant comparison of various legal traditions, governance structures, and policy agendas is made possible by the selection of these jurisdictions.

4.3.2 Legal parameters

For the purpose of establishing a framework that is consistent across jurisdictions, the Comparative Review of Law and Policy will conduct an examination of the various legal systems in a number of different countries. To facilitate comparisons among the various jurisdictions while also respecting the relevant laws and regulations of those jurisdictions, we can establish a standard set of legal parameters for all jurisdictions regarding privacy protection, surveillance powers, methods of enforcement, judiciary oversight, coverage of cybercrime, cross-border cooperation, and technology that can adapt to changing laws and regulations. These parameters allow for a structured comparison of the way each jurisdiction balances its national security goals with its citizens' privacy rights while avoiding the need for unnecessary technical or theoretical detail.

4.4 Method of Analysis

Using legal qualitative methods to study the interactions between national security and privacy in this modern digital world has led to an examination of how laws and case law are used to define the ways in which we protect our rights and privacy, and how they evolve over time across different jurisdictions (e.g., countries, states, etc.) and interpretive authority. This will allow for a systematic process of understanding how statutes (laws), judicial thought (reasoning and interpretation), and development of law in different regions (countries, states, etc.) interact.

4.4.1 Legal interpretation

The legal interpretation technique is employed in examining constitutional provisions, statutes, rules and regulations concerning cybercrime, surveillance, data protection, and national security. The legal interpretation process utilises a method for interpreting the language, scope and intent of legal texts to identify how laws address digital threats and safeguard fundamental rights.

In this research study, legal interpretation is applied to examine :

- The agreement between the United States Constitution and the states on the protection of liberty, and privacy through reasonable limitations
- Cyber and Data Protection Statutes
- The Authority given to State Authorities to conduct Surveillance and/or Intercept
- Legal Protections and Accountability Structures

This Methodology evaluates whether Current Laws sufficiently balance National Security with Privacy and assists with identifying whether there are Ambiguities, Limitations or Gaps in Existing Legal Frameworks.

4.4.2 Case law comparison

Judicial precedents from various jurisdictions serve as comparative case law to show how Courts from multiple regions understand and interpret Cyber Law and Privacy Principles within their respective realities worldwide. By analysing via a comparative analysis of such decisions by Judicial Authorities, it is possible to evaluate how Courts are applying the principle of proportionality and a Human Rights-Based framework when evaluating matters of Surveillance, Data Collection and National Security.

The Court of Justice of the European Union has rendered a number of judgments in relation to surveillance and data protection. Meanwhile, similar issues have also arisen in US and UK courts as they relate to cybercrime, digital privacy, and national security. In conducting this analysis, the objective is to examine to what extent the courts provide protection of civil rights and allow for legitimate security measures, as expressed in similar and contrasting ways by the courts of Europe and the USA/UK, as expressed in a comparative case law analysis.

Chapter 5

NATIONAL LEGAL FRAMEWORKS ON CYBERCRIME

The laws and policies pertaining to cybercrime in a few chosen jurisdictions are compared in this chapter. It evaluates different regulatory approaches, best practices, and enforcement mechanisms adopted by various states. The comparative perspective helps identify strengths, weaknesses, and lessons that can inform more effective cybercrime regulation.

5.1 Cyber laws in India:

Even while the internet and e-commerce were developed to facilitate quick and simple communication, they also subtly offer several chances for engaging in illicit operations. It is the responsibility of the authorized scheme to make rules to safeguard people against illegal action when it breaches their legal rights. The most significant area of the law that is directly related to everyone is criminal law. It is true that the finest criminal laws are those that criminalise as little as possible. As a result, when cybercrime became widespread in society, effective criminal laws were needed to stop it. The new realm of cyberspace has been created by information technology. The 21st century created this planet. It connects the world and creates a global village, yet it is not like a physical world. As a result, the legal system's workload grew. As a safety state-owned, it is the state's responsibility to safeguard its inhabitants online as well. As a result, the legal system must control cyberspace activity. Since it is a global issue rather than a national one, current cyber laws are transnational in character.

The Information Technology Act mainly deals with e-business/e-commerce regulations, introduced to the Indian legal system in the early 2000s while also recognizing some types of cybercrime. However, since the Information Technology Act establishes the authorities and regulations which govern digital signatures, many cybercrimes do not fall under this legislation; rather it is primarily a way in which to regulate the way in which 'digital' evidence can be collected and used by law enforcement agencies when investigating 'traditional' crimes. As such, many computer-related offences will likely fall under the Original Indian Penal Code (IPC) which covers many criminal acts, including those considered traditional forms of crime. Nonetheless, diverse methods are used to perpetrate cybercrime; some changes are needed to address the technical side. Consequently, the legal system enacts the internet law. Among these nations, India is one that is vigilant about potential cybercrimes[98].

5.1.1 Information Technology Act,2000:

The “Information Technology Act of 2000’s”, India's establishing law, regulates the usage of computers, computer networks, computer systems, and electronic data and information. Cybercrime, digital signatures, network service provider liability, and electronic authentication are only a few of the many themes covered by this act. According to the Act's Preamble, its goals are to make it easier to file documents electronically with government agencies and to offer lawful acknowledgment toward connections made via electric information exchange and further electric communiqué techniques, which are collectively referred to as "electronic communication." Substitutions to “paper-based communication and information storage techniques” are used in these transactions.

On the 22nd of December 2008, the Information Technology Amendment Bill, 2008 was approved by the Lok Sabha. It was subsequently confirmed by the Rajya Sabha on December 23, 2008. The President's consent to this bill was obtained on February 5, 2009 and this bill became effective as of October 27, 2009. The purpose of the Information Technology Act of 2000 was threefold: first, it facilitated the processes of government; second, it protected the

Indian IT industry from external threats; and third, it served as a deterrent against the rise of cybercrimes. The Act also sought to improve India's security standards for the benefit of the nation abroad. The amendment was made to take into account security problems that have emerged since the original legislation was passed, as well as advances in information technology, and to address issues that the original bill did not address. The "Information Technology (Amendment) Act 2008" removed Sections 91, 92, 93, and 94 from the original Act. There are two schedules, thirteen chapters, and ninety sections in the "IT Act of 2000". Sectors III plus IV were removed by the "Information Technology (Amendment) Act of 2008".

The term "electronic signatures" has replaced "digital signatures" in an attempt to create the Action further technologically unbiased. A novel definition of "communication device" has been introduced, which defines it as any device used for text, video, audio, or image transmission or reception, including cell phones, PDAs, or a combination of both.

Section 67 of the "Information Technology Act of 2000" consumes be there amended to increase the maximum fine "from Rs. 100,000 to Rs. 500,000" and decrease the maximum sentence from five to three years in prison for publishing or finding pornographic material online. Furthermore, Sections 67A through 67C are now included. The intermediary is required to keep records for a time specified by the government and in a form and manner requested by the government as set out in Section 67C. The penalties for the publication/transmission of child pornography and sexually explicit conduct of a child via an electronic medium are contained in sections 67A & B. As part of the amendment made recently, a modified version of 69 now gives the government with the added authority to use any computer resource to encrypt or monitor the information due to the increased threat posed by terrorist groups to the nation. Two new sections, 69A and 69B, permit the government to restrict access to any information gathered via computer resources and disallow the gathering of stats/information from computer traffic for cybersecurity purposes [86].

5.1.1.1 Nature of the I.T. Act, 2000:

It is mainly passed to documented and enable ecommerce and not to rule cybercrimes, but the Act describes few crimes and drawbacks. Chapter of the act deals with crimes and the penalties and the authorities regarding adjudication. These two chapters of the I.T. act deals with certain cyber-crimes. Chapter IX focus upon the given important attributes: Adaptable conduct in its own unique way; evidence-based rather than unlawful civil legislation; Instead of established civil courts, arbitrating officials are trusted with the settlement process

These officers are required to be knowledgeable about the rules and IT or to have legal expertise

- Civil court authority is granted to arbitrating officials
- The proceedings performed by these officers are to be construed as judicial records
- It is crucial that compensation be provided at market rate for losses or disappointments.

This feature suggests that since the chapter only deals with civil courts, there aren't many sections that deal with the authority to implement the outcome. If the IT Act falls within any criminal law's penal delivery, it may also register under those regulations if it is supplied with contracts for civil responsibility. This means that not every cybercrime is covered by this statute. It does, however, seek the backing of conservative criminal law. Because cybercrime is not as unique as predicted offences. The India Cyber Crime Act outlines various offences and their corresponding penalties including computer source document interference as described in Section 65 of this legislation. Section 65 discusses Computer Source Paper Interference: "Whoever knowingly destroys, modifies or obscures any system source code that is required to be maintained or continued in use as part of an operating system/Computer Application/Network Application/Computer Application by providing such services when indicated by way of receiving or accepting from others via email or other digital communication medium/cybercriminal activity, shall be liable for the punishment of custodial sentence for a term not exceeding 3 years with the possibility of further extension of up to 2 lakh rupees or both."

The IT Act's penal section addresses the act of concealing or modifying the source of a system. This offense pertains to the unauthorized use of another person's information without their permission or in violation of the agreement. The punishment for this offense is imprisonment for a period of up to three years. This section attempts to prevent individuals from taking action to erase, change or destroy the programs that are installed on the system or make them unusable by the individual who owns the programs. Regardless of whether the act was committed with intent or malice, the penalty may be up to three years in prison or a fine of up to two lakh rupees. This section of the Act was enacted to protect companies from potential harm caused by the breach of confidentiality of their sensitive information. To do this, companies need to maintain a record of their source code (the code written by programmers). In some circumstances, it is difficult for companies to prove that the source code is their property, since an ex-employee may take the code to another company. However, if the company has recorded its source code, it will be easier to identify the perpetrator.

There are further section 66, 67, 70 etc. which deals with the offences as like hacking the computer or offence of indecent publication which are in electronic form. Section 65 to 75 of the IT Act deals especially with the cybercrimes and the sentences for that, but these are not the all forms of the cybercrime. Whole these offences handle along the illegal act however it is similar to the much of the conservative offense, where in the computer is either device or board while obligating that offense. The Information Technology Act, 2000 defines a number of cybercrimes; these are sometimes referred to as "Cyber Violence" and "Indecent Material on the Internet." The Act provides a legal framework for prosecuting offenders in the Indian legal system. Rules and regulations outlined in the Information Technology Act and other legal acts are also classified as Cyber Crime violations under Cyber Laws:

1. Information Technology Act, 2000

2. Information Technology (Certifying Authorities) Rules, 2000

3. Information Technology (Security Procedure) Rules, 2004

4. Information Technology (Certifying Authority) Regulations, 2001 As the demanded act also could not accomplish the requirement of time and cyber safety is facing the issue also the implementation is not being possible since because of few technical issues. Hence, the Information Technology Act is radically corrected within year 2008.

A Section 81 now includes a clause saying that the Act's provisions take precedence. This clause states that nothing in the Act prohibits the exercise of any rights provided under the 1957 Copyright Act. Notification of decisions made in accordance with the 2000 Information Technology Act. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 were implemented in 2011.

A set of rules known as the Information Technology (Electronic Service Delivery) Rules of 2011 governs how information technology is used to provide electronic services.

- Information Technology (Guidelines for Information Diaries) The Rules of 2011 are a series of regulations that govern how information diaries utilise technology.
- Information Technology (Cyber Guidelines) Information technology use at cyber cafes is governed by a set of rules known as the Rules of 2011.
- The Cyber Appellate Tribunal (Salary, Allowances, and Others Terms and Conditions of Service of the Chairperson and Members) Rulings, 2009 are a set of regulations that control the pay, benefits, and other terms and conditions of service for the chairperson and members of the Cyber Appellate Tribunal.
- The Cyber Appellate Tribunal's Rules (Procedure for Investigating Chairperson and Members' Misconduct or Incapacity), 2009
- The Information Technology Act of 2009 (Procedure and Safeguards for Preventing Public Access to Information),

- The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 regulate the interception, monitoring, and decryption of information.
- The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009, regulate the monitoring and collecting of information technology.
- Information Technology (Electronic Records and Digital Signatures) The Rules of 2004 regulate the use of electronic records and digital signatures.
- The Information Technology (Security Procedure) Rules of 2004 regulate the usage of information technology.
- Information Technology (Other Standards) The Rules of 2003 regulate the usage of information technology.
- The Information Technology (Certifying Authority) Regulations of 2001 regulate information technology certification.
- The Information Technology (Certifying Authorities) Rules were implemented in 2000.

5.1.1.2 Overview of Other law Amended by the IT act,2000:

The IT Act of 2000 updated the Indian Penal Code of 1860 and the Indian Innovation Act of 1872 to reflect the fast-changing technology world. On October 17, 2000, fixed supplies were integrated under the Information Technology Act of 2000, which was illegal in India. The Indian Penal Code is implied by the functional criminal law of India because the various crimes that fall under this category are too similar to those that fall under the category of cybercrime. The only difference between the two types of crimes is the technology used to commit them, so changes are necessary to bring these crimes under the purview of this code. The amendment adds a new phrase to the Indian Penal

Code, "will to exercise operative execution through supplies handling along with such type of crimes that are going to be committed by means of information technology."

The Information Technology Act of 2000 covers a wide range of offences, including publishing sexual content, sending violent emails, defiling secrecy, and mitigating along workstation bases. The Indian Penal Code already recognizes all of these unlawful acts as crimes. Considered similarities might be discussed in the following ways: similar crimes also occur below the IPC.

- Sending threatening messages by email Section 503 IPC
- Sending defamatory messages by email Section 499 IPC
- Forgery of electronic records Section 463 IPC
- Bogus websites, cyber frauds Section 420 IPC

5.1.1.3 New cybercrime under I T Amendment Act, 2008:

Many cybercrimes that were not specifically covered by the IT Act of 2000 are now covered under the IT (Amendment) Act of 2008. Sending violent or misleading communications (s. 66A), delivering stolen computer reserves (s. 66B), stealing someone's identity (s. 66C), lying via personation (s. 66D), and defilement of confidentiality (s. 66E) are only a few of the additional criteria that this Act adds to section 66. All of these items raise concerns about isolation rights, but since they will be violated in a number of ways, they must be included in the Act. Section 66 F adds the new crime of cyber assassination, which carries a penalty that might result in lifetime incarceration. Section 66 F covers any act intended to cause anxiety or intimidate India's unity, integrity, security, or autonomy, such as launching denial-of-service attacks, starting computer pollutants, gaining unauthorised access to a system resource, stealing confidential information, any facts that could harm India's autonomy or unity, the security, friendly relations with other public order, states, morality, decency in relation to contempt of court, slander or provocation to a crime, or for the benefit of any imported nation, group of people.

These crimes are more serious since new techniques of communication will now be used to commit crimes against the country. The prescribed punishment for other offences listed under Section 66 is often up to three years and a fine of one or two lakhs. These offences are known and may be released on bond. This won't demonstrate a fundamental preventative element for cybercriminals. Additionally, according to the new Section 84C, an attempt to obligate a crime is also punishable by imprisonment for a term that may be up to half of the longest term of imprisonment specified for that offence. In accordance with the new Section 84B, wrongdoing to obligate a crime is typically made indictable along with the retribution delivered for the crime under the Act.

Section 67A makes it illegal to distribute content that contains sexually explicit activity. This offence carries a five-year jail sentence and a fine of up to 10 lakhs. This delivery was required to prevent MMS assaults and video voyeurism. According to Section 67B, child pornography and sexually explicit acts or behaviours by children are punishable by up to five years in prison and a fine of up to 10 lakhs. This has been a good development as it makes collecting and browsing child pornography a disciplinary offence. Sentence for revealing up of knowledge into break of legal contract under Section 72 is augmented from two years up till five years along with from one lakh to five lakhs or both. This will frighten commission of such offense. By virtue of Section 84 B person who back up a cybercrime will be penalized with sentence provided for that crime under Act. This delivery will play a preventive role and prevent instruction of machination related cybercrimes. Additionally, sentence for effort to constrain crimes is provided within Section 84 C, which will be disciplinary with one half of the stretch of release settled for that particular crime or that like fine as provided or both.

The amendments to the I.T. Act of 2008 include huge changes. A lot of the changes have introduced how various offences that can result in prosecution will now be classified as Cyber Crimes and will now fall under the terms of the Indian Penal Code. It should be noted that, depending on the way Cyber Crimes are committed, it would not be appropriate for the amendment to be applied to every type of cybercrime because they do not have the same

attributes as traditional crimes and can be committed using a variety of means. Hence, the system may serve as an instrument for committing a Cyber Crime or, in certain instances, be utilized as a target for a Cyber Crime.

5.1.1.4 Indian Penal Code, 1860:

The IPC was altered by Section 91 and the First Schedule of the IT Act of 2000. The Information Technology (Amending) Act, 2008 replaced Section 91 and transferred the provisions of the Indian Penal Code to Part III [87]. The following changes have been made to the Indian Penal Code:

- "Amendment to Sec.4" – In section 4, clause (2) will be followed by the following clause: (3) Any person who deliberately targets an Indian computer from outside India. ii) The explanation will be replaced with the following one: (a) Any act committed outside of India that would be punishable under this code if committed inside India is referred to as a "offence." (b) The definition of "computer resource" is given in clause (k) of subsection (1) of section 2 of the Information Technology Act of 2000.
- "Amendment of Section 118": The phrase "voluntarily conceals, by any act or illegal omission, the existence of a design" in section 118 should be replaced with "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design."
- "Amendment of Section119": In subsection 119, the phrase "voluntarily conceals, by any act or illegal omission, the existence of a design" will be replaced with "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design"

The terms "electronic signatures" must be used whenever the term "digital signatures" appears in section 464.

- Offences covered under IPC and Special Laws:
- Theft of Computer Hardware:-Secs. 378, 379 IPC

- Obscenity:-Secs. 292,293,294 IPC, Indecent Representation of Women Act
- Insult to modesty of women:- Sec 354 of IPC.
- Criminal Intimidation by E-mail or Chatting:-Secs. 506, 507 IPC
- E-Mail Abuse, On line Defamation:-Secs.500, 509 IPC
- Forgery of electronic records:-Secs 463, 464, 468, 469 IPC
- Cheating with Bogus websites and cyber frauds:-Sec 420 IPC
- Extortion via Web-Jacking:-Sec. 383 IPC
- Receiving stolen property:-Sec.411 IPC
- Criminal Misrepresentation:-Secs.403, 404 IPC
- Criminal Breach of Trust:-Sec.406 IPC
- Email spoofing:-Sec 463 IPC

5.1.1.5 Criminal Procedure code:

In cognizance of an offence punishable under Sections 417, 419 and 502 of the Indian Penal Code, except upon a complaint made through the individual distressed through the crime," according to Section 198 B of the Criminal Procedure Code, which was introduced shortly after Section 198 A125. Additionally, several concepts like "crimes" and "computer resource" have been defined more thoroughly in the Indian Penal Code, drawing inspiration from the IT Act of 2000. It demonstrates that India is successful in dealing with emerging IT challenges. The Copy Right Act has undergone several changes due to the dispute that some information should be protected as private property and achieved through "Ownership." Cyber law is given a value in the administration of justice, taking into account the needs of people today.

5.1.1.6 Indian Evidence Act, 1872

Another procedural law is the Law of Evidence. The Indian Evidence Act 1872, which has been in effect since September 1st, 1872, is regarded as the Law of Evidence for India and has

undergone several amendments. Before the Indian Evidence Act of 1872 went into effect, Indian courts in Presidency cities adhered to the rules of English law on evidence. In moffisil, Mohammedan law of evidence was followed for sometimes by British courts. Codified Act Of 1855, draft bill of law of Evidence in 1868 and finally a new draft prepared by Mr. Stephan was passed as Indian Evidence Act and the same came into force in 1872. These are some of the phases through which Indian Evidence Act emerged in 1872 and the same is in force as present.

- Section 92 and the Second Schedule of the IT Act of 2000 included amendments to the Provisional Act. Section 92 of the Information Technology (Amendment) Act, 2008 was repealed, and the provisions pertaining to the Indian Innovation Act were transferred to Part IV of the amendment[88].
- Changes to Section 3 - The terms "digital signatures" and "digital signatures certified" will be substituted with "electronic signatures" and "electronic signatures certified" in the paragraph at the end of Section 3 pertaining to the interpretation clause.
- New Section 45A – Opinion of the Electronic Device Examiner 45A: The opinion of the examiner of electronic evidence mentioned in section 79A of the Information Technology Act, 2000 is a pertinent fact when the Court must form an opinion on any matter pertaining to any information transmitted or stored in any computer resource or other electronic or digital form. Explanation: An analysis of electronic devices is necessary for the objectives of this section.
- Changes to Section 47A - The terms "digital signatures" and "electronic signatures" should be substituted in section 47A, and "digital signatures certified" should be substituted with "electronic signatures certified."
- Changes to Section 67A – The phrase "electronic signatures" in section 67 A will be replaced with the terms "digital signatures."

5.1.2 DPDP act, 2023:

The Digital Privacy Act (DPDP Act), 2023, which provides Indian citizens more control over their personal data and privacy, is a turning point for the collection and monitoring of public health data. Therefore, by employing a "Tiered Framework" approach to Managing Personal Data, the act gives the Indian court system more opportunities and challenges regarding the processing of Personal Data in India. In this sense, the goal is to offer an additional foundation for safeguarding individual privacy while permitting the honest and legal handling of personal data. The Digital Data Protection Directive created a number of extensive laws and regulations pertaining to data protection. The first major piece of legislation addressing the Digital Era was the Information Technology Act 2000 ("IT" Act). The Information Technology (Intermediary Guidelines) Rules 2011 came after the IT Act. which sought to address some of the Data Protection issues at that time. However, as technology continued to advance, so too did the way Digital Data was collected & used, and many existing laws were unable to adapt to the fast-paced changes associated with Modern Digital Data Use.

The DPDP Act closes a big gap left by its predecessors. This act was written to provide a full legislative framework that will address the many components of data protection. The act's writing is based on input from years of meetings and discussions with various stakeholders regarding their views on data protection.

Definition of Personal Data (Section 2(t)):

Any information that could be used to directly or indirectly identify a person is deemed personal data under the Act's broad definition. As part of this definition, the Act includes all data collected by the courts about judges, lawyers, witnesses, parties and all court personnel. This means that how the courts perform their duties with respect to this personal data will be determined by what they think the definition of "personal data" is according to the Act.

Data Processing (Section 4):

The Act regulates how Personal Data may be collected, stored, used, disclosed and destroyed. As a result of their large volume of Personal Data, Courts will also need to ensure that the Act is being complied with. In order to comply with all of the obligations set forth in the Act, Organizations must obtain valid consent from Individuals prior to collecting their Personal Data, only collect they data necessary to fulfil the purpose(s) for which it was collected, and only collect Personal Data for purposes that are permitted by law.

Data Principal Rights (Section 11-15):

According to the Act, individuals have the right to access, edit, and delete their personal data. Therefore, courts must also provide sufficient procedures that comply with this Act, so that they may respond to any of these requests in a timely and appropriate fashion. Courts may also have to create new procedures or amend existing ones in order to protect the rights of those individuals whose data is the subject of interest.

Data Transfers (Section 16):

Data Protection legislation (the "Act"), as it applies to India, restricts the movement of personal data beyond the borders of India. The sharing of personal information in India between Courts and law enforcement agencies for investigation purposes or Court related matters will be affected by the Act's restrictions on transferring data.

Data Breaches notification (Section 8):

According to the new law, whenever there is a data breach or a threat of a data breach, both the affected individuals and the Board (data protection authority) must be notified. Courts are very popular targets for cyber-attacks and experience high rates of data breaches that will be subject to the security requirements and respond to the Act.

Accountability and Enforcement (Sections 13):

The Act states that both the Authority and the people impacted by a data breach will be subject to the provisions set forth by the Act. Additionally, because Courts face the risk of

cyber-attacks and data breaches, the Act requires all parties impacted by the breach implement reasonable security measures and incident response plans.

Implications for Court Accessibility:

- Even though one of the primary goals of the DPDP Act is the protection of individual data and their associated rights, there are numerous effects it will have on access to the Courts.
- As courts remain committed to complying with the DPDP (Data Protection & Digital Privacy) Act, they are attempting to increase the public's trust and confidence in the – Judicial System (by increasing the public's trust and confidence in its ability to provide justice).
- As a result of limiting the ways in which Courts may utilize Data pursuant to the DPDP (Data Protection and Digital Privacy) Act, Courts are likely to increase their productivity due to increased opportunities for utilizing efficient Data Management methods; this increased utilization of efficient Data Management methods will also reduce the administrative burden on the Courts' operations and improve the Courts' ability to efficiently deliver Court Services.
- Difficulties Involved in Sharing Court Data with Other Agencies: Data sharing between courts and various Other Agencies will be limited by the DPDP Act. Therefore, this limitation will make it harder for courts to manage the legal process effectively.
- Finding an Equitable Balance of Privacy Rights and Access to Justice: The DPDP Act will require Courts to develop creative methods of balancing the need to protect individuals' Privacy Rights and also provide them with equitable access to Justice. Therefore, courts will maintain the integrity of an individual's Personal Data while providing access to Public Information through this innovative balance [89].

Historical Development and Scope of the Digital Personal Data Protection Act, 2023 (India)

The creation of the DPDP is a pivotal moment in developing India's emerging digital laws in relation to growing fears regarding the security of someone's individual privacy rights and protection against the misuse of personal data via technology.

For years, the laws regulating the protection of personal data in India have been patchy at best, focused primarily on corporate entities instead of the individual. In addition, they have provided a limited amount of protection for how individuals use their personal data. While both the IT Act and subsequent implementations of IT Rules did have some protections associated with personal data and privacy in India, the range of protections provided prior to the promulgation of the DPDP Act were quite limited and were not adequately enforced, leaving the majority of the Indian population unprotected from the abuses of their personal data by commercial actors.

The Final Drafts of the Proposed Legislative Bills had to go through Multiple major Revisions due to the ongoing discussions and debates concerning Data Localization, State Surveillance Exemptions, Consent Mechanisms and Private Sector Roles. The withdrawal of the “Personal Data Protection Bill, 2019 (PDPB, 2019)” and the “Data Protection Bill, 2021 (DPB, 2021)” demonstrates the challenges to reaching regulatory agreement within India in an environment that is Changing Rapidly.

The Indian Parliament recently passed the DPDP on August 2023, which will put into place a statutory Framework Regulating the use of Digital Personal Data for both the Private and Public Sectors, and that will focus primarily on Consent-Based Processing and Purpose Limitation. The Structure of the DPDP Act will be much more Streamlined compared to prior Bills.

In the DPDP Act, there are Definitions and concepts of Data Principals and Data Fiduciaries, empowering individuals through agency and accountability regarding their data Processing activities. Additionally, the DPDP Act specifies that the only lawful actions for Processing of Personal Data in India are based on Consent or are classified by GRE Forms as Legitimate Use as defined in the DPDP Act. Furthermore, the DPDP Act will provide enforcement rights for

individuals that include Access to Personal Data, Correcting Data, Requesting Erasure, and the right to file a Grievance.

Another significant element of the DPDP Act is creating the Data Protection Board of India, which will have the jurisdiction over compliance with the DPDP Act, adjudication of breaches of the DPDP Act, and imposition of penalties for violation of the DPDP Act. The DPDP Act also includes significant Financial Penalties for Violating the DPDP Act, thereby signaling an intention toward greater enforcement of the DPDP Act, as compared to the IT Act. Along with providing Protections for Personal Data, there are several significant exemptions to State governmental authority to process Data. Specifically, for National Security purposes, for the preservation of Public Order, and for the Prevention of Crime. There is considerable Academic debate regarding whether there are sufficient safeguards to protect privacy from excessive surveillance and unlawful actions from Leadership, especially given the current constitutional law framework that has established Privacy Rights for every person in India.

5.1.3 Judicial Interpretation:

The authoritative explanation provided by courts to determine the extent, significance, and application of a law while settling legal disputes is known as judicial interpretation[5].

Judicial interpretation is particularly significant in cyber law because,

- Technology advances more quickly than laws.
- New digital behaviours are frequently involved in cybercrimes.
- Courts must strike a balance between public order, national security, and individual
- Rights, Previous laws, including the IT Act of 2000, include legislative gaps.

5.1.3.1 Principles of Judicial Interpretation:

1. Literal Rule

The plain and usual sense of the terms used in the statute is how judges read the law under the literal rule. used in cases where the definitions of terms like "computer system" and "electronic record" are explicit under the IT Act.

2. Golden Rule

The golden rule allows courts to change the precise meaning of words to avoid absurd or unjust outcomes. If taken literally, it might make legitimate internet behaviour unlawful.

3. Mischief Rule

This rule emphasises on identifying the problem or misconduct that the law was intended to prevent and interpreting the statute in a way that suppresses that misconduct. utilised to address emerging cybercrimes that aren't expressly addressed by the law.

4. Purposive Interpretation

Instead of interpreting laws strictly according to their words, courts do so in accordance with their goals and purposes. frequently used in situations pertaining to national security, data protection, online expression, and surveillance

5. Harmonious Construction

Courts interpret conflicting law provisions in a way that upholds each without contradicting one another.IT Act clauses pertaining to constitutional rights: IPC-compliant cyber laws

6. Constitutional Interpretation

Courts interpret cyber laws in light of fundamental rights, particularly:

- “Right to privacy”
- “Freedom of speech and expression”
- Judicial interpretation has played a crucial role in shaping the understanding of data protection and privacy within modern legal systems, particularly in jurisdictions where comprehensive statutory frameworks emerged only recently. Courts have gradually

expanded the meaning of personal liberty to include protection over personal information, digital identity, and informational autonomy in response to technological change.

- In early judicial reasoning, privacy was treated as an implied and limited aspect of personal liberty rather than an independent right. At times, the Courts have favored State interests - public order, safety & Crime Prevention - supported by granting law enforcement broad latitude for issues related to Surveillance, Data Collection, and Interception of Communication.
- As a result of the changing nature of privacy and its contextual nature, the interpretation of the right to privacy by the courts was also influenced. With the increasing use of technology in our everyday lives and the ability to collect, organize, and analyze the personal data of individuals from various sources (e.g., social media), the courts began to recognize that the accumulation and analysis of individuals' personal data has the potential to provide insight into an individual's private life and, therefore, should be afforded the same level of legal protection as traditional means (i.e. written, audio, etc.) of obtaining personal data.
- The development of case law has illustrated the judicial reasoning that any type of interference with an individual's ability to enjoy his or her own private life has to have a legal rationale, a legitimate objective, and be in a fair manner that is proportional to the benefits derived from the interference with the individual's ability to live a private life. Therefore, the judicial interpretation of the right to privacy provides a framework for creating organized limitations on governmental power through the establishment of procedural safeguards, accountability and transparency in the governing regulatory framework for collection, processing and storage of personal data.
- Judicial decisions about how to protect privacy rights are evolving to recognize the risks associated with unregulated digital surveillance, including potential alteration of behavior through surveillance, as well as profiling individuals and restricting their rights

to free expression. Courts are now beginning to recognize that the use of bulk collection of personal data has an adverse chilling effect on people exercising their freedom of speech and the right to associate freely with others and to maintain a level of anonymity while interacting online. This shift judicial interpretation toward a communal democratic virtue and an individual privacy right.

- Another significant change in how courts view data protection is that it is seen as an ongoing process rather than a one-off event. As such, courts have stated that organizations must take steps to ensure there is a minimization of data collected and that data is only collected for a specific purpose and that organizations will implement measures to protect the data through the entire lifecycle of the data from the time it is collected until the organization no longer has that data.
- Additionally, courts are recognizing the extent to which the digital world is a global marketplace and, therefore, how location-specific laws do not achieve their intended purposes when it comes to protecting privacy for individuals who use digital technologies worldwide. For this reason, courts are calling for both the creation of uniform regulations to provide international enforcement of privacy protection laws and encouragement for countries to work together to protect the privacy rights of all people.
- Overall, the approach of interpreting privacy and data protection in the courts has elevated the status of these issues from 'periphery' to 'foundational'. The connection between the constitutional values of society and the technological world of today is being established by courts through policies concerning privacy and data protection. In the digital age, as our online world continues to grow and develop, the role of judicial interpretation in protecting individual liberties from harmful technology will become increasingly important [90].

5.2 Cyber law in US:

The United States follows a predominantly **security-centric and enforcement-oriented approach** to cyber law, shaped largely by national security concerns, technological innovation, and federalism. In the United States, Cyber Crime Law is not governed under a single statue that comprehensively covers the entire issue of Cyber Crime. Rather, Cyber Crime Law is determined through a fragmented, Sector-Specific body of Cyber Crime Laws that cover Cyber Crime as well as Privacy, Data Protection and Cyber Security. The "Computer Fraud and Abuse Act (CFAA)", passed in 1986, serves as the primary Federal Law regulating Cyber Crimes. The CFAA makes it illegal to access a computer without the owner's permission, steal data, hack into someone's computer and related Cyber Crimes. While the CFAA has been used to prosecute many Cyber Criminals, there have also been many criticisms associated with the CFAA including vague definitions, over-criminalization and the wide discretion given to prosecutors regarding the enforcement of the CFAA. After the attack on September 11, 2001, the U.S. Cyber Crime Law was significantly expanded in response to the increased focus on National Security resulting from that attack through the implementation of the USA PATRIOT Act. This Act gives many additional powers of surveillance to U.S. Intelligence Agencies to collect, store and transmit through Foreign Intelligence (FI) all Electronic Communications and Digital Metadata in the name of National Security. The Foreign Intelligence Surveillance Act (FISA) and the FISA Amendment Act also provide additional powers of surveillance to the U.S. Government through Electronic Surveillance, often in secret before the U.S. Foreign Intelligence Surveillance Court (FISC). Data protection regulations in the United States are sector-specific because there isn't a national statute similar to the "General Data Protection Regulation (GDPR)" of the European Union. For example, the "Children's Online Privacy Protection Act (COPPA)" controls the application of COPPA to children's online information, the "Gramm-Leach-Bliley Act (GLBA)" controls the application of GLBA to financial data, and the "Health Insurance Portability and Accountability Act (HIPAA)" controls the application of HIPAA to health data. Because there isn't a clear framework for securing customers' private information,

the way consumer privacy laws prohibit people from having their private information viewed without their consent has been wildly uneven.

In 2018, Congress passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which provides significant new authority for law enforcement agencies to obtain data located outside of the United States pursuant to U.S. Federal law. While this new authority is beneficial in that it will help law enforcement to combat cybercrime, it creates significant issues related to sovereign rights, privacy and conflicts of law.

Overall, U.S. cyber law policies prioritize protecting the nation's security and providing more effective means of gathering intelligence, but often at the expense of strong protections for individuals' right to privacy. Although there is judicial oversight of U.S. cyber law, it is generally very limited, and as such, the debate regarding the relationship between the U.S. constitution, the proportionality of invasive measures and the degree of transparency required when using digital surveillance continues.

5.2.1 The Computer Fraud and Abuse Act (CFAA), 1986:

The CFAA Act of 1986, "codified at 18 U.S.C. 1030", amended the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984" to expand the types of computers covered by the law and the illegal conduct. This prospect became more apparent as the potential use of computers to commit other types of crimes became increasingly apparent. The most well-known federal law in the US that deals with computer hacking and cybercrime is the CFAA. 189 assaults on "protected computers," which are defined as "computers (a) used in or affecting an information exchange and analysis system (b) used in or affecting a financial institution or the United States government and the action constituting the offence affects that use." Seven hacking techniques are listed in the CFAA as being illegal under federal law. The first four clauses specifically mention unauthorized access. Getting information on national security (18 U.S.C. 1030(a)(1)): Knowingly obtaining information with the intention of harming the United States or benefiting a foreign nation by using unauthorized computer access or exceeding

authorized access limits; knowingly giving that information to a third party who is not authorized to receive it or withholding it from the party who is authorized to receive it [91].

Using a computer to access and obtain information (18 USC 1030(a)(2)) is the deliberate entry into a computer without authorization or by going beyond what is allowed and obtaining data from a secure computer, a financial record, a US department or agency, a consumer reporting agency, or a financial institution. Trespassing on a government computer is defined as purposefully and illegally gaining access to a non-public computer of a US department or agency or a computer whose actions affect how the government utilizes it (18 U.S.C. 1030(a)(3)).

The fifth statute is U.S.C. 1030(a)(5). It emphasizes that "knowingly inducing the transmission of a program, information, code, or instruction and, as a result, intentionally cause damage without authorization to a protected computer" is illegal. "Willfully accesses a protected computer without authorization and recklessly causes damage," or "willfully accesses a protected computer without authorization and causes damage and loss." The first section of the law forbids using code to intentionally damage a protected machine. Because of this, the CFAA is essentially the only federal statute that can be used to punish offences involving the use of dangerous software. Since malicious software is merely computer code, it should be made clear that it is not criminal in and of itself. The use of malware on a computer or system and the use of damaging software to gain unauthorized access to systems are prohibited in the United States and many other countries. Regulations pertaining to computer hacking in the US and other countries concentrate on situations where malicious software was utilized to obtain unauthorized access to computers or systems.

The sixth and seventh clauses of 18 U.S.C. 1030 (a)(6) and (a)(7) prohibit the exchange of passwords and the use of computers for blackmail. Unauthorized purchases, sales, or exchanges of passwords or other information that can be used to access any computer used by the federal government or for interstate or international trade are prohibited by 18 U.S.C. 1030(a) (6). Demanding money or other assets from computer owners to stop data loss or damage is

prohibited by 18 U.S.C. 1030(a)(7). Finally, it should be noted that any effort or conspiracy to commit any of the seven crimes mentioned above is prohibited by Section 1030(b). According to Brenner191, 1030(a)(4), 1030(a)(5), 1030(a)(6), and 1030(a)(7) are the statutes that prosecutors are most likely to use because they cover the more general offences, while the other sections concentrate on more specialised computer types or cybercrime, such as financial institution computers rather than all protected computers.

Both the harm inflicted and the number of past convictions have an impact on the severity of the sentence when found guilty of these charges. The minimum term for trespassing operations intended to gather information for national security is ten to twenty years. The maximum penalty for using a computer to get private information is ten years in jail and/or a fine if the offender is charged with multiple crimes or committed the offence for financial or personal advantage. In a similar vein, trespassing on government-owned computers carries a maximum sentence of one year in prison, a fine, or ten years if the behavior was linked to other consequences for (a)(5) can range from a fine to a sentence of two years to life in prison, depending on whether the deed resulted in death.

The perpetrator may receive a term of up to ten years in jail if they are proven guilty of several offences or if the data is worth more than $5,000. Last but not least, violations of (a)(7) may result in penalties and/or up to ten years in jail if the perpetrator has a criminal record.

Additionally, state laws forbid the use of code for unauthorized access and computer hacking. When the Computer Crimes Act was passed in 1978, Florida became the first state to pass legislation outlawing "computer hacking". The primary subjects of computer crime laws in the United States are computer hacking and unauthorized access. 192 Aggravated hacking, which is defined as unauthorized access that results in additional criminal activity, such as copying or destroying data, is classified as a felony in most states, while simple hacking, which is defined as unauthorized access without causing harm to the system or engaging in additional criminal behavior, is classified as a misdemeanor. In some countries, a single statute forbids unauthorized access, regardless of whether further criminal activity occurs. States also vary in whether they

passed new legislation to more precisely describe the traits that distinguish computer hacking and cyberstalking or if they deemed these acts unlawful under pre-existing statutes against theft and robbery [3].

Historical Development and Scope of the CFAA act:

The CFAA of 1986 constitutes the cornerstone of cybercrime legislation in the United States and represents one of the earliest legislative efforts globally to address computer-related offences. The enactment of the Computer Fraud and Abuse Act (CFAA) was made in response to the vast growth in technology in the late 1970's and early 1980's. Computers were becoming a major component of how governments operated, banks operated their financial systems, and how countries implemented their national security systems. Before the CFAA was passed, the criminal laws that applied in the U.S. were not created to criminalize activities that could be defined by a computer. Early examples of hacking, unauthorized access to data, and data manipulation provided numerous examples which illustrated that the existing criminal laws which provided protection against the physical entry someone could make on to someone else's property could not be applied against the unlawful entry made by someone over a computer system. Because of this, in order to provide an avenue through which to prosecute computer-based misconduct, Congress added the CFAA as an amendment to the existing federal fraud statutes to explicitly make a criminal offense to misuse a computer. When first passed, the CFAA was very narrowly focused solely on protecting federal government computers and financial institutions. At that time, the primary reason for the enactment of the CFAA was to deter unauthorized access to government systems with sensitive classified materials on them and to stop espionage, sabotage, and financial fraud. The initial penalties included anyone accessing a computer "without authorization" or accessing a computer "exceeding authorized access" who intended to acquire confidential government information or financial information.

The CFAA has evolved over course its passage through a series of amendments that greatly broadened the scope of the Act. The broadening of the CFAA occurred with each of the amendment Acts (1989, 1994, 1996, 2001, 2008). It is believed that the essential transformation

of the CFAA into a broad Cybercrime Statute occurred with the 1996 amendment that extended protections to computers utilized in interstate or foreign commerce, essentially allowing any computer that was connected to the Internet to be covered by the CFAA.

After the terrorist attacks on September 11, 2001, the USA PATRIOT Act was passed to provide for additional penalties for violations of the CFAA and to enhance the ability of law enforcement and intelligence agencies to share information, as well as to enhance the ability of law enforcement to surveil activities that were suspected to be related to terrorist activity. Additionally, while the perception of Cybercrime as a threat to National Security grew, it was also recognized that Cybercrime could also represent an Economic Threat.

The CFAA prohibits many different types of Cyber Misconduct including: hacking, accessing data without authorization, the transmission of malicious code, denial-of-service attacks, and the trafficking of passwords. Additionally, the CFAA allows for criminal and civil liability to be imposed upon individuals and corporations as a result of violations of the CFAA. This dual enforcement mechanism has caused the CFAA to be frequently used in Courts as an enforcement mechanism.

The CFAA has been subject to Critical analysis from many perspectives, including Courts, legal scholars, and those advocating for civil liberties. In particular, the ambiguous wording of "unauthorized access" and "exceeding authorized access" in the CFAA, has been a point of contention between Courts. Another concern is the different interpretations by Courts regarding whether the CFAA's prohibition against violating website terms of service is overreaching (in the broad sense) or whether it is overly restrictive, thus resulting in over-criminalization of conduct by an individual.

There are also concerns among opponents of the CFAA due to the increasing media attention on cases involving journalists, academics and activists, regarding the CFAA potentially infringing upon First Amendment rights, hindering ethical hacking practices, and working against lawful academic research. In addition, some argue that the CFAA's ambiguous language gives prosecutors too much discretion and creates unnecessary risk for the average internet user.

The CFAA's implementation and interpretation have significantly changed due to judicial interpretation. The US Supreme Court cases recently emphasized the need to balance law enforcement's duty of protecting the public with civil liberties (including due process and the First Amendment). The cases attempted to clarify the extent of the CFAA's intended scope.

The CFAA represents the primary legal framework the US government uses to prosecute cybercrime today in an ever-increasingly digital world. But even though this old law is still being used today, some experts feel it is too old-fashioned and should be reformed to reflect current technology trends such as Artificial Intelligence (AI) based attack vectors, insecure clouds, and international Cyber Crime operations.

The growth and development of the CFAA throughout its history specifically demonstrate how the Government has reacted to techno-terrorism from the standpoint of maintaining National Security. While the CFAA has fulfilled a necessary protective role for our Digital Information Infrastructure up until now, it continues to rely on outdated constructs and definitions. Current discussions on the CFAA indicate that more reforms to this law will ultimately make it easier to understand, enforce fairly, and bring it into alignment with our rapidly changing technological reality and also our Civil Liberties.

5.2.2 Patriot Act:

The USA PATRIOT ACT has a very broad scope and nature. The act is well-known for its provisions to combat the "war of terrorism" globally and to intercept and obstruct terrorism in the United States, but it has also been able to invalidate several fundamental civil liberties. The law "contains over 150 Sections and 10 Titles ..." (Gale, 2005: 215). However, unless the US Congress approves a renewal, 1/101 of the acts expire on December 31, 2005, due to "Sunset"20. Title II of the Act contains the most hazardous provisions that generate issues with civil freedoms. For this reason, the Act's "Grandfather Section" refers to the parts under Title II. Despite the fact that this title consists of just 25 portions [92].

5.2.2.1 Historical Background of the Act:

The Historical background of the act is represented in Table 5.1 and Table 5.2 represents Nature and scope of the Act.

Table 5. 1 Historical Background of the ACT

Period / Year	Law / Event	Purpose / Context	Impact on Civil Liberties	Relevance to Patriot Act
1798	Alien and Sedition Acts	Enacted during fear of war with France; aimed to control aliens and suppress political opposition	Restricted free speech, deportation without due process	Set precedent for suppressing liberties in the name of national security
1917	Espionage Act	Passed during World War I to prevent anti-war activities and espionage	Criminalized dissent, anti-war speech	Basis for criminalizing speech linked to national security
1918	Sedition Act (Amendment to Espionage Act)	Strengthened restrictions on speech critical of the government	Severe suppression of First Amendment rights	Demonstrated expansion of surveillance and punishment powers
1947	National Security Act	Post-WWII restructuring of defense and intelligence (NSC, CIA)	Institutionalized security-first approach	Created permanent national security framework
1950	McCarran Act	Cold War fear of communism	Allowed detention and surveillance of suspected subversives	Expanded intelligence powers later mirrored in Patriot Act

1978	Foreign Intelligence Surveillance Act (FISA)	Regulated electronic surveillance for foreign intelligence	Allowed secret courts and classified surveillance	Patriot Act significantly expanded FISA powers
1996	"Anti-Terrorism and Effective Death Penalty Act" (AEDPA)	Passed after Oklahoma City bombing	Limited habeas corpus, expanded deportation	Direct legal predecessor to Patriot Act
September 11, 2001	9/11 Terrorist Attacks	Massive intelligence failure and national trauma	Public fear enabled acceptance of strong laws	Immediate trigger for Patriot Act
October 26, 2001	USA PATRIOT Act enacted	To prevent terrorism and enhance intelligence coordination	Expanded surveillance, reduced privacy protections	Most comprehensive security law in U.S. history
2005 onwards	Amendments & Renewals	Review and extension of controversial provisions	Partial restoration of oversight, sunset clauses	Shows continuing debate on liberty vs security

Table 5. 2 Nature and Scope of the ACT

Aspect	**Provisions under the Act**	**Explanation / Significance**
Nature of the Act	Anti-terrorism and national security legislation	Enacted to prevent, detect, and punish terrorism, especially after the 9/11 attacks
Legislative Character	Emergency and fast-track legislation	Passed with minimal debate, reflecting urgency and national fear

Extent of the Act	Over 150 sections under 10 titles	Covers surveillance, immigration, finance, intelligence sharing, and criminal law
Focus on National Security	Strengthening domestic and international security	Prioritizes national security over individual liberties
Surveillance Powers	Enhanced electronic, wire, oral, and digital surveillance	Allows roving wiretaps, internet monitoring, and interception of communications
Foreign Intelligence Surveillance (FISA)	Expansion of FISA authority	Surveillance allowed on citizens and non-citizens with secret court approval
Access to Records (Section 215)	Access to business, library, medical, and financial records	Law enforcement can obtain records without probable cause
Information Sharing	Greater coordination among intelligence and law-enforcement agencies	Removes barriers between FBI, CIA, NSA, and immigration authorities
Immigration Control	Detention, deportation, and monitoring of aliens	Broad definition of "terrorist" enables preventive detention
Detention Provisions	Mandatory detention of suspected terrorists	Habeas corpus and judicial review significantly restricted
Financial Surveillance	Anti-money laundering and terror financing controls	Banks required to report suspicious transactions
Border Security	Enhanced border checks and biometric identification	Strengthened passport, visa, and entry-exit controls

Presidential Powers	Expanded executive authority	Limits judicial review and increases executive discretion
Judicial Oversight	Reduced transparency and ex-parte proceedings	Courts often excluded from meaningful review
Sunset Clauses	Certain provisions subject to expiration	Some sections reviewed, amended, or renewed periodically
Civil Liberties Impact	Curtailment of privacy, free speech, and due process	Raises constitutional concerns under the First and Fourth Amendments
Global Reach	Extra-territorial application	Applies to foreign nationals and international financial transactions
Victim Protection	Compensation and support for terrorism victims	Provides financial aid and legal support to victims
Overall Scope	Comprehensive restructuring of security law	Transforms criminal justice, surveillance, and immigration frameworks

5.2.2.2 Application of the Act:

However, the Act's implementation is rather different. Unlike other laws that apply exclusively to the administrative authority or sovereignty of the state. It considers every incident of terrorism and recommends appropriate action. This implies that it applies to all forms of terrorism and terrorist acts both domestically and internationally. This law may apply to any individual, group, or even country that engages in any of the activities specified in the act. It discusses both lawful and unlawful combatants, as well as enemy combatants in general, in addition to terrorism and terrorist-related acts. It covers everything from custody and deportation of offenders to interception and obstruction. Additionally, it recommends actions for any connections between terrorists and their groups. Thus, the act's scope is quite broad and includes all forms of terrorism and its connections. Even though the US has a variety of

appropriate laws to combat terrorism and related activities, such as immigration laws and antiterrorist activities legislation, the current law has been able to outperform them all. It is interesting that this act keeps track of all terrorist actions and any associated terrorist activities, even when the US is not involved in any way. While terrorist activities happen more frequently in Asia or Africa, this act will also be the agency in charge of collecting evidence and making final decisions concerning these crimes.

5.3 Cyber laws in UK:

The UK is implementing a rather balanced approach to cyber laws that seeks to balance the requirements of national security with civil liberties and the requirements of judicial oversight. The CUK Cyber Law is based on both tradition of Common Law and the “United Kingdom's treaty” obligations under the “European Convention on Human Rights (ECHR)”.

The “Computer Misuse Act 1990” is the main legislation that deals with cybercrime. It makes it a criminal offence to have unauthorized access to computer material, to unauthorizedly alter computer data and to use the Internet to commit fraud against others (e.g. to steal somebody's credit card information). The Act has been updated several times to keep pace with new threats posed by cybercrime such as “Distributed denial-of-service (DDoS)” attacks and serious cyber-offences. One of the most important parts of the UK cyber law is the Investigatory Powers Act 2016 (IPA), commonly referred to as the "Snooper's Charter". The IPA provides a detailed legal framework for how the state may intercept and store the data of citizens, as well as a mechanism to collect large amounts of data (bulk data) that could also be used by the state for a variety of purposes, including combating terrorism/serious crime. The IPA uses a dual lock authorization mechanism2701 for surveillance (the same type of mechanism as the U.S.), meaning that both an executive (government) and a judicial authority must approve the enforcement of this law. Under the “General Data Protection Regulation (GDPR)” of the United Kingdom, and the Data Protection Act 2018, the United Kingdom has maintained GDPR-like protections. The two laws focus on data minimization, lawful processing and transparency; and individual rights, but both the UK GDPR and the Data Protection Act, 2018 provide an exemption for national security, which is subject to review.

Particularly because the European Court of Human Rights has ruled against unmitigated or unrestrained surveillance activities, the UK places a high value on proportionality, accountability and judicial review. To summarize, the UK framework surrounding cybercrime and cyber security attempts to balance the need for security and the need for privacy along with

accountability. The UK framework represents a much more moderate model that incorporates extensive monitoring capabilities, as well as legal protections and supervisory mechanisms.

5.3.1 Computer Misuse Act:

There have been a number of growing illegal incidents of unauthorised access to computers. Due to this, many offences were created with the "Computer Misuse Act 1990 (CMA)" and as a result, hacking has increased greatly; in fact, it is still increasing. A significant amount of damage is being done by computer misuse and the number and seriousness of the vulnerabilities available for hackers continues to expand. There are some instances where criminal behaviour has created a loophole in the law, including in the prosecution of certain Denial of Service attacks [93].

The world began to recognise the possibility of computer crime in the 1980s. Lawyers were starting to look at problems as computer security experts were developing sets of security standards. The Scottish Law Commission released a report on computer crime the next year after publishing a memorandum on the subject in 1986 (Scottish Law Commission, 1986, 1987). Many of the difficulties that would eventually be addressed by the Computer Misuse Act were mentioned in these early investigations, but the field was developing so quickly that the Scottish findings had little immediate impact. The UK Government was awaiting the Law Commission's findings before taking any action in England, where the commission was farther behind schedule in its discussions.

But when a member of parliament placed highly on the ballot for a private member's bill and declared that a Computer Misuse Bill will be introduced, the timeline for action was compelled. The government supported the measure rather than taking control of it, which is unusual for this type of legislation. The Law Commission report (Law Commission, 1989) was completed quickly and released on schedule, and its suggestions served as the foundation for the legislation. The CMA 1990 was the final outcome.

Three sections comprise the Act's crimes. Unauthorized access is covered in the first, least serious section; computer usage to commit additional crimes is covered in the second; and unauthorized modifications are covered in the third.

It came to the conclusion that, rather than using the criminal damages act for this purpose, it would be safer to catch all such activities under the new law. However, there may be situations in which computer abuse also results in physical harm, in which case the criminal damage act's provisions would be applicable.

5.3.2 Data protection Act:

The first data protection bill in the UK was presented to the House of Lords in December 1982, but the 1983 general election prevented it from being passed. One of the first significant data protection laws in history, the Data Protection Act of 1984, was created from a second bill that was filed in July 1983. A new system for storing and processing "information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose" was established by the 1984 Act. Data users, or individuals who possess data, were required for the first time to register with the Data Protection Registrar's office, a supervisory body. There are two aspects to the new legislation: the first is a compensation scheme for victims of breach by the public; the second is criminal prosecution against offenders. The second aspect (criminal prosecution) is only applicable where there is no registration with the Data Protection Registrar for the automated processing of 'personal data' by an individual [94].

The application's approval from the Registrar allowed it to post in the Register which was open for public viewing. The data user committed an offence under law by processing the data if they had not registered. The data subject may request access to any of his/her personal data held by the data processor and the data processor must respond within 40 days of the request. The courts or the Data Protection Registrar will penalize those who

fail to comply. Additionally, a data subject may be entitled to compensation from the data processor if they experienced harm as a result of data loss, inaccuracy, or unauthorized disclosure. The data subject also had the right to have any inaccurate information kept by the data user corrected or erased. In court, both of these rights were enforceable.

5.3.2.1 Data Protection Principles under UK Law

Based on the Data Protection Acts and policy reports, the following principles form the foundation of UK data protection law:

- Fair and lawful processing
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Security safeguards
- Transparency and data subject rights
- Accountability and monitoring
- Restrictions on transborder data transfers

Purpose Limitation: Personal data must be gathered for a specified, legal purpose and cannot be utilized for any other reason without the required authorization. Data should only be utilized for the purpose for which it was gathered.

Authorized Access Only: Only authorized individuals who require the information for the intended purpose may access personal data. Personal information should only be viewed or used by those who are authorized.

Data Minimization: To accomplish the targeted goal, only the bare minimum of data should be gathered and kept. It does not gather more personal data than is necessary.

Separation of Identity (Anonymization): Whenever possible, personal identity should be kept apart from the data in systems used for statistical or research purposes. When complete identification is not necessary, personal identify should be concealed.

Transparency and Right to Know

- People have the right to know what information is kept about them.
- Individuals should be informed about:
- What data is held about them
- Who holds it
- Why it is being used

Security Safeguards: To prevent unauthorized access, misuse, loss, and destruction of data, appropriate organizational and technical security measures must be put in place. Personal information needs to be protected from hacking and abuse.

Monitoring and Accountability: Systems should include monitoring features to identify and stop security lapses or personal data abuse.

Storage Limitation: Personal information should not be retained for longer than is required to fulfil the reason for which it was gathered.

Accuracy of Data: Personal information must be correct, current, and updated when mistakes are found.

Fair Use and Value Judgments: When evaluating people based on their statistics, caution must be exercised. People shouldn't be unfairly judged or harmed by data.

From the late 1960s until the Data Protection Act was passed in 1984, data protection law in the UK underwent significant development. In response to a series of private members' bills supporting varying degrees of privacy regulations, the UK government commissioned two significant investigations in the 1970s. Ten recommendations for the management of personal data were included in the first, the Younger Report on Privacy (1972). The extent of those

suggestions may still be seen in the work of the present Information Commissioner's Office, 25 years after the Lindop Report was published. The growing reliance on gathering personal data and the realisation that unrestricted collection and distribution of personal documentation and data could potentially jeopardise individual privacy led to the development of data protection laws in the UK and other European nations.

To address these issues, the Swedish section of the International Commission of Jurists (ICJ) hosted the Nordic Conference of 1967 in Stockholm. Through study and lobbying legislators, particularly in international organisations like the United Nations and the Council of Europe, the International Court of Justice (ICJ), an autonomous body of judges and lawyers, promoted the advancement of human rights. They listed 10 rights in their declaration on the essence of the right to privacy. Certain rights had a stronger connection to data protection than others. The latter three individual rights must be protected from:

The Interference with his correspondence.

- Misuse of his private communications, written or oral.
- Disclosure of information given or received by him in circumstances of professional confidence.

They were highly persuasive despite having no legal status, and they played a significant role in the national debates that raged throughout the 1970s about what privacy and data protection meant. None of the private members' bills that were introduced in both chambers between 1961 and 1972—some pertaining to particular aspects of privacy and others to privacy in general—were passed into law. In 1961, the House of Lords introduced the first privacy bill with the intention of "protecting a person from any unjustified disclosure related to his private matters and giving him legal rights in that regard."One Other bills made an effort to regulate databases, either manually or electronically.

However, it was not until the Data Protection Act of 1998 that both electronic and manually processed data were ultimately controlled in the United Kingdom.

Information that can be used to identify a living person is covered by the Act. Included are names, dates of birth, anniversaries, residences, phone numbers, fax numbers, email addresses, and more. It only applies to data that is kept in a relevant file system or that is meant to be stored on computers or other devices that function automatically in response to instructions given for that purpose. The information commissioner, who has been appointed as the government official in charge of executing the Act, requires persons and organisations that possess personal data to register. Data collection was restricted by the Act.

A person's personal information may only be gathered for one or more authorised, stated purposes, and it may not be used for any other purposes. Concerning the purpose or purposes for which they are processed, personal data must be appropriate, relevant, and not excessive. Through Article 8 of the ECHR and the ECHR cases, the Council of Europe had a key influence on the EU data protection system. Aside from that, Convention No. 108 and Recommendation R (87)15 play a role in the safeguarding of the comprehensive convention.3Article 8 of the European Convention on Human Rights is the data protection knight in shining armour. The importance of Article 8 cannot be overstated, as, before the Lisbon Treaty, the CJEU did not rule on data protection issues until 2009.4 Before the treaty's implementation, the court was restrained by then-established EU rules in this area owing to the constitutional divide, which was subsequently abolished by the treaty. While the European Courts were constrained by the previous EU and EC Treaties, the ECHR's expertise allowed it to develop key principles in this field.

Article 6 of the Treaty on the Functioning of the European Union and Article 6 of the Treaty on the Functioning of the European Union and Article 6 of the Treaty on the Functioning of the European Union and Article 6 of the Treaty on the Functioning of the European Union and Article 8 of the Convention on the Rights of the Child and Article 7 of the Convention on the Rights of the Child established an all-encompassing fundamental right in the EU. Furthermore, the extent of the convention's rights will be identical to the basic rights of the EU that correspond to the ECHR.6 The interpretation of Articles 7 and 8 of the Charter is therefore

done while keeping in mind the principles adopted by the ECHR while remaining within the scope of Article 8, which deals with data protection and privacy.

5.4 Cyber law under European Union:

The three jurisdictions reviewed, the European Union (EU) has developed the most rights-focused and harmonised approach to cyber law. This set of laws is based upon fundamental rights, including “privacy and data protection”, found in the “EU Charter of Fundamental Rights”.

There are comprehensive regulations regarding the “collection, processing, storage, and transfer of personal data, and the GDPR” is fundamental to EU cyber law. Among other requirements, organizations which collect and/or progression individual files necessity obtain explicit consent from affected individuals and must restrict the usage of their data to the resolution for that data was collected. As such, data controllers and processors have responsibilities that include establishing accountability, complying with a 'data minimisation' requirement, and providing individuals with enforceable rights, including “access to their data, the right to have erroneous data corrected, the right to have their data erased, and the right to transfer their data to another organization”. The NIS Directive requires certain entities to ensure the security of their operations and the fulfilment of cybersecurity responsibilities on an ongoing basis and is supplemented by the NIS2 Directive. Together, these directives have built upon the existing cybersecurity framework to further strengthen the EU's position in terms of protecting both public and private-sector systems and networks from cyber threats.

The EU is more constrained than America when it comes to regulating how citizens can be monitored because the EU adheres to strict guidelines about what can be done and how much. The CJEU has rejected many of the unreasonable practices concerning data retention and large-scale monitoring of EU citizen's communications, and stressed that any Surveillance measures in the name of “National Security shall” always respect the “Right to Life, Liberty, Personal Privacy, Dignity and Security protected” by the “Charter of Fundamental Rights of the European Union”.

The EU is also a prominent player shaping International Cyber Governance and developing the International standards of Data Protection, including encouraging partnership efforts between jurisdictions based upon the presentation of “Human Rights standards”.In sum, the EU model places Privacy, Accountability, and Standardization & Protecting Human Rights at the forefront of its goals. The EU Model has set a comparison standard for the development of democratic Cyber Law within the World.

5.4.1 GDPR (General Data Protection Regulation):

GDPR - The General Data Protection Regulation is the highest level of data and privacy protection Laws globally. GDPR applies to all Organizations across the globe that collects or use the data of EU citizens irrespective of where those organizations are located regardless of whether they were established or approved by the EU. Organizations that violate either of these standards will be punished heavily by way of fines up to tens of millions of euros, beginning to take effect on 25 May 2018. Serious penalties will be imposed on those who violate the GDPR's security and privacy requirements [95].

In order to pursue data privacy, GDPR's new data protection policy has concentrated on starting a constant process of creating improvement measures across international organizations. R4 claims that the EU's GDPR is a crucial step in encouraging the sustainability of consumer data use across various platforms. The policy is more effective and sustainable than the previous data protection regulations. International data protection disputes between businesses may have decreased as a result of the new data regulation. As a result, R7 and R8 contended that GDPR has concentrated on starting a proactive viewpoint and strategy in building resilience towards the digital data concerns that affect information security and privacy through a number of papers. "There has been a chance to enhance individual privacy rights while simultaneously raising awareness of the impact of local and state actors in organizations." For instance, end result, the “EU's GDPR policy” to regulate data privacy has changed how organizations use and acquire redundant consumer data while limiting possibly unauthorized

usage, which has decreased consumer lawsuits in businesses regarding data privacy violations. Furthermore, the emergence of digital technology has made information privacy a contemporary idea that has made it necessary to regulate both local and international organizational practices. According to R9 and 10, the EU's GDPR has led to a uniform worldwide standardization of organizational management practices for consumer digital data. "Aiming to harmonies global data usage and transfers, the GDPR is a combination of various data policy practices." In order to provide a comprehensive policy tool for adoption and implementation across different organizations, the GDPR takes into account a number of EU directives[10].

5.4.2 Historical Evolution of the General Data Protection Regulation (GDPR)

The historical development of the “GDPR” is closely linked to the evolution of “privacy and data protection” as fundamental rights within the European legal order. The origins of data protection in Europe can be outlined posterior to the “post-World War II period”, when the protection of individual dignity and autonomy emerged as a core concern of human rights law. Provided by the 1950 “European Convention on Human Rights (Article VIII)”, the civil rights to Seclusion have existed since 1950. The beginning of “Automated Data Processing” in the Late 1970's spurred European States to pass their main group of records defense laws as a reaction to the increased efficiency made available through this new technology; Germany, Sweden and France were some of the earliest countries to enact national statutes for regulating Computerized Personal Data, specifically to prevent abuse of Power by Government Agencies. Acceptable security of the privileges of beings regarding access and dealing out of this kind of documents was established with these first-generation laws, thus establishing this as a separate and distinct type of Legal Interest within the “European Union Framework”.

In 1981, the signing of the "Council of Europe Convention 108," or more commonly referred to as the "Data Protection Convention," became the First Legally Binding International Treaties

to Establish Data Protection as an International Issue and represented an important milestone in the development of Data Protection Laws within Europe. The Core Principles created by Convention 108 have served as a foundation for Additional Projects by the European Union and include: Conditions under Which Data May Be Lawfully Processed, Quality of Data, Restrictions on the Use of Data, and the Rights of Individuals to their Data processed under these guidelines.

"Directive 95/46/EC, the EU's Data Protection Directive", was adopted in 1995 with the intention of establishing a "single data protection law for the EU" and permitting the free flow of private data between member states within the internal market. The directive was viewed as a major advancement, although member nations applied it extremely differently; This is because it was a directive and not a regulation. This created differences in how the directive was applied and enforced which caused fragmentation and uncertainty around legal issues.

By the early 2000's, technological growth—including, among other things, the development of the "internet, social media, cloud computing, and big data analytics"—demonstrated shortcomings in the "Data Protection Directive adopted in 1995". The complexities associated with the handling private information increased, as did the number of countries involved as well as the focus on the business side of personal records. As growth of "big data analytics, mass collection, profiling and tonight", employees of private companies as well as the Government, were increasingly concerned with the manner in which the private and government organizations would use personal data. The European Commission recognized that the rapid technological changes would require a complete overhaul of the "EU data protection laws" and began a process of re-evaluation of "EU data protection laws in 2012". This would involve legislative reform to modernize the laws, provide stronger individual rights, create greater uniformity in enforcement, and accommodate for the changing digital environment. Following extensive consultation, negotiation and deliberation surrounded by "EU institutions, member states and other interested parties", the GDPR was officially adopted in April 2016.

Compared to the 1995 Directive, the GDPR was adopted as a Regulation, so there is no requirement for National Transposition and is enforceable across all Member States. Thus, moving to a legally harmonized and strongly enforced model the GDPR was officially launched on the 25th of May 2018 and replaced the "Data Protection Directive". The idea of records defence has evolved from a symbolic framework to a new paradigm of Information security as a vital factual under the GDPR. Individual rights have significantly increased as a result of this shift. Examples of individual rights include: right to information, right to get information; right to access, right to view your personal files; right to rectify, right to correct errors in your information held by an organization; right to delete (also called 'right to be forgotten'); right to restrict processing, right to have limited contact(s) with an organization during certain times; right to transfer (the information collected by or shared with an organization); and right to complain.

The Enforcement Mechanism of the GDPR has also been significantly strengthened. Independent Supervisory Authorities have been empowered to enforce compliance, and Non-Compliance is now subject to the imposition of Significant Administrative Fines. As a result of the above changes, Data Protection moved from a largely symbolic framework to a Robust Regulatory Regime with substantial Economic and Legal Impact. One of the most significant aspects of the GDPR is that the regulation extends its reach outside of the EU to all non-EU entities that collect or use individual's personal data for their own purposes. The extraterritorial application of the GDPR has had a substantial influence on developing world-wide standards around statistics safety and helped to create convergence between EU and non-EU standards.

Over the years, the GDPR has developed as a response from the European Union to meet the demand for isolation and information security as a result of the rapid changes occurring due to technology, globalization, and the increasing awareness of surveillance and abuse of technology over individuals' rights to privacy. The GDPR can be considered as the culmination of a process that has taken many decades of experience and is now recognized as the world's best example of regulatory compliance for individual privacy based on the principles of human rights.

5.4.2 NIS Directive in EU:

The first horizontal framework rule at the EU level designed to safeguard networks and information systems surrounded by entirely "EU member states" is the "NIS Directive". The emergence of cybersecurity threats, events impacting vital services, and significant cyberattacks endangering Member States' national infrastructure and the operative of the "EU internal market" led to the creation of this regulation.

The main advancement in EU Cybersecurity law is through the founding of a common legitimate basis within which all Associate Countries are to observe by the "NIS Directive" for "securing network and information systems" across all Associate Countries. The establishment of individual obligations on Digital Service Providers, and those who provide security to Critical Services through the creation of a common cyber resilience approach, are among the numerous benefits that the NIS Directive provides to Member States in growing their ability to defend themselves from cyber assaults. The transition to a unified Governance arrangement between the "EU and Member States" for Cybersecurity as a result of the establishment of the "European Network and Information Security Agency (ENISA)" supports this transition from individual governance arrangements for Cybersecurity to the establishment of a common governance structure for Cybersecurity across the EU [96].

The primary objective of the "NIS Directive" is to:

- Make vital digital and physical infrastructures more resilient to cyberattacks.
- Ensure that vital services continue throughout the EU.
- Encourage Member States to collaborate and exchange information.
- Set minimal security and incident reporting requirements.

The "General Data Protection Regulation" that departed within consequence on "May 25, 2018", goals to guarantee the unrestricted effort of private information within the "EU" while also protecting entities through concern toward handling that information. The release of the two legal texts, GDPR and NIS Directive, were in very close proximity to each other; the GDPR

on April 2016, and NIS Directive on July 2016. However both legislative processes did occur independently and in parallel. Between 2013 and the date of their release only one reference was made in a European Data Protection Supervisors opinion regarding NIS Directive.

History of NIS Drective:

The EU NIS Directive has been an important step in establishing a comprehensive approach to cybersecurity and protecting critical digital infrastructure in the EU, reflecting a shift away from viewing the problem of cyber incident risk to individual users and the risk to critical service delivery or the stability of economies and the national security of "individual EU Member States". In the early 2000s, as the "EU" became more reliant on digital systems for its economic integration and public service delivery, increasing concerns were raised about how susceptible EU Member State critical infrastructures may be to cyber attack. The EU Cyber Security Strategy (2013) was one of the first documents to outline the need for EU Member States to work together and develop a coordinated and harmonised approach to cyber security. Prior to this document, individual EU Member States had developed their own national strategies and laws and regulations to address their respective challenges regarding technologies related to cyber security on a continuing basis over many years (e.g., through the EU Digital Single Market initiative). After several significant and widespread cyber incidents that impacted extensively and affected almost all of the sectors considered to be critical to society (e.g., financial, energy, telecom, etc.) as well as the government, it became clear that cyber threats would continue to exist unless they were dealt with as cross-border issues and could not be delimited by an isolated response from individual EU Member States. In response, the "European Commission" proposed the "**NIS Directive in 2013"** as portion of a wider determination to enhance the flexibility of "network and information systems" across the Union. The proposal designed to establish a communal baseline of cybersecurity obligations for Member States while respecting national security prerogatives.

In July of 2016, after long discussions with the EU and other organizations, the NIS Directive was agreed and accepted by EU Parliament, becoming the first legally binding legislation for

EU based upon Cyber Security. Unlike the previous soft law instruments that had been used previously, there are now legally binding obligations on both public and private sectors. The "NIS Directive" required all Member States to laid in residence "national cyber security solutions" (strategies), appoint a national competent administrative body to oversee their "national cyber security development" and make a "national Computer Security Incident Response Team", and participate in the European Union Cyber Security Cooperation Framework. The idea was to assist with the improvement of the countries cyber security foresight and readiness, sharing of information with other agencies, and as a result coordinate their responses to cyber incidents.

One of the most beneficial parts of the NIS Directive was a separation of all effected entities into two classifications, "Operators of Essential Services (OES)" and "Digital Service Providers (DSPs)". OESs contained energy, transport, banking, healthcare and water supply sectors; whereas DSPs contained "online marketplaces, search engines and cloud service provider (CSP)". Both of the classes of service will have to lie on place appropriate cyber security specific security processes and also have to report cyber incidents of significance.

The employment of the "NIS Directive" highlighted a significant number of deficiencies in relation to the flexibility allowed to individual country Governments regarding the identification of OES and definition of the security measures to be implemented. The "NIS Directive" didn't offer adequate clearness or guidance on how to meet the security goals. In addition, the limitations of each individual Member state to enforce their specific regulations or to report significant cyber incidents further reduced the overall efficiency of the "NIS Directive".

The quick development of ordinal equipment and the escalating number and sophistication of cyberattacks necessitated a reevaluation and revisitation of the "NIS Directive" framework; the emergence of cloud computing, IoT, AI and increased reliance on supply chains has introduced new cybersecurity threats that were not fully considered in the original Directive.

Now graceful of the above mentioned challenges, the “European Union” began a process to analyse and amend the “NIS Directive” leading to the establishment of the “NIS2 Directive in 2022”; In contrast to the “NIS Directive”, the NIS2 expands the scope of Cyber Regulations by adding more sectors, granting the Member States greater supervisory authority over their Member States and further erecting stricter compliance measures such as the ability to impose administrative penalties against non-compliant entities.

The NIS Directive's historical development indicates that the EU has been moving from a number of disjointed national cyber policies to a unified and harmonious governance model; additionally, the NIS Directive represents the EU's acknowledgement of the significance of cyber security towards the operation of the European Interior Marketplace, in addition to the “defence of major rights, national security, and the EU's collective security”. The NIS Directive is viewed as an important foundational point for EU Cyber Law and provides a basis for establishing an all-inclusive Cyber Security Framework that will be able to deal with future Cyber Threats in this ever-more connected World.

5.5 Key Statutes and Regulatory Provisions of India, US, Europe and UK:

In table 5.3 represents, the Regulatory Provisions of India, US, Europe and UK

Table 5. 3 Key Statutes and Regulatory Provisions of India, US, Europe and UK

Country	Principal Legislation	Key Provisions	Enforcement/Regulatory Body
India	"Information Technology Act, 2000 (Amended 2008)"	Covers electronic signatures, cybercrimes (hacking, obscenity), and intermediary liability.	"Ministry of Electronics and Information Technology (MeitY)"; Cyber Appellate Tribunal.
	DPDP Act, 2023	Regulates personal data processing, data principal rights, and breach notifications.	Data Protection Board of India.
USA	"Computer Fraud and Abuse Act (CFAA)", 1986	To "protected computers," fraud, and damaging systems with code.	Department of Justice (DOJ); FBI.
	USA PATRIOT Act, 2001	Broadens surveillance powers for "war on terrorism" and monitoring of digital communications.	Department of Homeland Security (DHS); NSA.

UK	CMA Act, 1990	Defines offenses for unauthorised access, data alteration, and access with criminal intent.	National Cyber Crime Unit (NCCU).
	"Data Protection Act (DPA)", 1984/2018	Establishes principles for fair, lawful, and secure processing of personal information.	"Information Commissioner's Office (ICO)".
Europe	"General Data Protection Regulation (GDPR)"	The global gold standard for data privacy. Includes "Right to be Forgotten," strict consent rules, and data portability.	"European Data Protection Board (EDPB)" and "National Data Protection Authorities (DPAs)".
	NIS2 Directive, 2022	Enhances cybersecurity for critical sectors (energy, transport, health).	"European Union Agency for Cybersecurity (ENISA)" and National CSIRTs.

5.6 Enforcement Challenges:

Judicial interpretation has changed the way that the CFAA has been implemented and applied over time. Through its focus on balancing both law enforcement's responsibility to protect communities (maintaining public safety) with individuals' civil rights (e.g., due process and freedom of speech), recent decisions from the “U.S. Supreme Court” have tried to define how far the CFAA applies. The CFAA serves as the key which the “U.S. Federal Government” deals with cybercrime in today's modern digital environment [12].

5.6.1 Jurisdictional and Cross-Border Challenges

As cybercrime is international in character, there will always be worldwide jurisdiction over all aspects of the crime. The criminal's country of origin, victims, and servers will likely span several countries and therefore be governed by multiple countries' national laws such as the “Indian IT Act 2000, United States CFAA 1986, United Kingdom Computer Misuse Act 1990, and the European Union Directives”. National laws provide the basis for jurisdiction over a country, but when a cybercrime occurs across national boundaries, the jurisdictional authority provided by the individual national laws is limited. In most cases, the only means to obtain assistance from a foreign country to investigate cybercrime are through Mutual Legal Assistance Treaties (MLAT), Extradition agreements, or Letters Rotatory. All of these ways to obtain assistance are also generally viewed as cumbersome, politically sensitive, and slow, which can result in significant delays in the sharing of evidence. As cybercrime is international in character, there will always be worldwide jurisdiction over all aspects of the crime. The criminal's country of origin, victims, and servers will likely span several countries and therefore be governed by multiple countries' national laws such as the “Indian IT Act 2000, United States CFAA 1986, United Kingdom Computer Misuse Act 1990, and the European Union Directives”. National laws provide the basis for jurisdiction over a country, but when a cybercrime occurs across national boundaries, the jurisdictional authority provided by the

individual national laws is limited. Cybercriminals exploit jurisdictional differences by routing their attacks through jurisdictions with weak or nonexistent cyber laws, or through jurisdictions that lack the capacity to enforce their laws. These loopholes provide a "safe haven" for cybercriminals and decrease the deterrent effect of all cyber laws, underscoring the need for countries to develop harmonized international rules of law concerning cybercrime.

5.6.2 Attribution and Evidentiary Difficulties

Attribution concerns figuring out who (or what) done it when it comes to cybercrime and is thus arguably one of the more difficult aspects of enforcement, due to the prevalence of various anonymising methods, encryption tools, VPNs, proxy servers, and dark web sites used to hide an offender's identity. In India, there is already a legal foundation for accepting electronic evidence as per the IT Act (2000) and CFAA, however courts are regularly faced with issues regarding the authenticity of electric proof; the integrity of electronic evidence; and the chain of custody of electrical indication. In addition, cyber criminals are able to commit crimes using automated techniques or artificial intelligence, which present a much higher level of difficulty for law enforcement agencies to determine culpability.

5.6.3 Rapid Technological Evolution

The speed at which cybercrime develops is far greater than the speed at which legislation does. The IT Act (2000), for example, was created when types of cybercrime such as ransomware-as-a-service, AI-assisted phishing emails and IoT attack vectors did not exist. Hence enforcement agencies have to rely on judicial interpretation of the current and outdated legal framework when prosecuting modern-day crimes. Emerging technologies such as AI blur the lines between civil liability, criminal liability and state-sponsored cyber operations. In Table 5.4, Emerging Cyber Threats vs Legal Coverage is presented**.** The ineffective laws result in a weakened capability to enforce future web crime prevention and leave courts as de facto lawmakers by default.

Table 5. 4 Emerging Cyber Threats vs Legal Coverage

Emerging Threat	Legal Coverage Status
Ransomware	Partial
AI-based attacks	Minimal
IoT exploitation	Inadequate
Deepfake fraud	Fragmented
APTs	Indirect

5.6.4 Institutional and Capacity Constraints

For effective enforcement of cybersecurity laws, agencies must have the necessary Digital Forensic Infrastructure, training, and coordination between departments. Most developing nations, however, do not have the required level of technical expertise.

Additionally, police forces are often using outdated technologies to investigate cybercrime (well before you could use software). Additionally, judges and prosecutors frequently do not understand how cyber offenses work; therefore, they will probably not understand what is being requested by the prosecutor. This leads to delays in procedural processes, weak convictions, and low numbers of reporting. Additionally, the limited capabilities of these agencies will create an environment of selective enforcement, where only those very publicized cases become the focus of investigations, and all other daily occurrences of cybercrime will go mostly unreported, or under reported, as it were. In Table 5.5, Institutional and Capacity Constraints is presented.

Table 5. 5 Institutional and Capacity Constraints

Constraint	Consequence
Lack of forensic experts	Weak investigations
Limited budgets	Poor infrastructure
Judicial skill gaps	Misinterpretation of evidence
Training deficits	Low conviction rates

5.6.5 Balancing Security and Fundamental Rights

In the enforcement of Cyber Law, there is a heavy reliance on surveillance, data interception, and blocking of content. While these methods can be justified under the pretext of National Security and maintaining Public Order; they still raise significant concerns around Constitutional Rights.

The laws in India's IT Act (Sections 69, 69A, and 69B) the USA's PATRIOT Act, and the Cybersecurity Laws created by the European Union has granted exceedingly large authorities to government entities, with little or no Judicial Oversight over their use; thus, opening themselves to possible misuse resulting in the potential for mass surveillance, censorship, and infringement upon an individuals' Civil Liberties [97]. In table 5.6, Measures vs. Fundamental Rights is generated. Courts are responsible for ensuring that actions carried out by enforcement agencies are compliant with (i) Necessity, (ii) Proportionality, and (iii) DUE PROCESS.

Table 5. 6 Measures vs. Fundamental Rights

Enforcement Tool	**Right Affected**
Surveillance	Right to privacy
Content blocking	Freedom of speech
Data retention	Informational autonomy
Monitoring	Due process

5.6.6 Compliance and Regulatory Fragmentation

Confusion will arise from the interaction of many regulatory frameworks that coexist in the current environment. This is evident in the EU where organizations must comply with both GDPR and NIS Directive compliance; even though they have some similarities there are also distinct differences in their respective compliance obligations.

Similarly, multinational companies struggle to comply with multiple regulatory frameworks regarding data localization, intermediary liability, and notification timelines for affected individuals due to the level of regulatory fragmentation; while these frameworks generate increased costs to comply with as well as differences in how they are enforced between the various jurisdictions. In Table 5.7, Jurisdiction and Key Compliance Focus is presented and Table 5.8 presented Enforcement Challenges Vs Legal Response.

Table 5. 7 Jurisdiction and Key Compliance Focus

Jurisdiction	Key Compliance Focus
India	Surveillance & data protection
USA	Security & national interest
UK	Unauthorized access & privacy
EU	Data protection & resilience

Table 5. 8 Enforcement Challenges Vs Legal Response

Challenge	Legal Response	Gap Identified
Cross-border crimes	MLATs	Slow process
Anonymity	Surveillance laws	Privacy conflict
Digital evidence	Evidence Acts	Technical gaps
Rapid tech change	Judicial interpretation	Legislative lag
Capacity limits	Training provisions	Resource shortage

5.6.7 Limited International Cooperation Mechanisms

On a global scale, the enforcement of cybercrime legislation is characterized by the fragmentation of the various laws, a "reactive" approach taken by most enforcement Bodies and extremely low levels of funding for both the law enforcement and judicial systems. Although many international cooperative agreements exist to facilitate communication and information exchange on cybercrime, the lack of an umbrella treaty that can be "enforced" in all participating

nations creates a situation whereby governments of various countries continue to have difficulty in coordinating the fight against cybercrime, frequently relying on informal, voluntary cooperation. Thus, many instances of cybercrime investigations lack the level of cooperation necessary to facilitate the compilation of a successful case.

The increased desire for cooperation has led many countries to create their own national and regional laws to address the issue of cybercrime based on the existing body of laws, but enforcement issues continue to prevent those laws from achieving their intended purposes. In order to effectively combat cybercrime, and enhance the ability to pool resources and knowledge in a coordinated manner, Governments of the world must continue to work to create a mechanism for improving international cooperation, establishing institutional capacity to effectively enforce the laws that have been enacted to combat cybercrime, develop technological solutions that will assist in responding to and preventing cybercrime, and ensure that individuals' rights are preserved so that the enforcement of cybercrime laws will be effective. Without the creation of such a treaty, it is likely that governments will continue to respond reactively rather than proactively to incidences of cybercrime.

As a result, there are still many countries that have extensive laws; but, globally, enforcement of those laws will continue to be reactive, fragmented, and poorly funded. To achieve a sustainable level of success for managing future cybercrime, there must be increased international collaboration, a commitment to respecting all types of human rights, improved technology capacity in countries to address areas of need, and the establishment of structures that allow for the evolution/development of effective Cybercrime Management Systems.

CHAPTER 6

COMPARATIVE ANALYSIS OF CYBER LAWS

The chapter focuses on how quickly advances in various technologies create new difficulties in regulating cybercrime. It identifies issues related to jurisdictional boundaries, responsibility for actions undertaken using technology, and how cyber resilience is affected by technology. It also addresses the vulnerabilities of Internet of Things (IoT) and concerns with artificial intelligence, as well as the risks associated with emerging technologies, such as deepfake technology, and the limitations of the current legal system in dealing with these risks.

6.1 Need for Comparative Legal Analysis

The international character of cyberspace is one of the reasons why there is a need to conduct Comparative Legal Analyses within the field of Cyber Law. In cyberspace, things such as Cybercrime, Digital Data, and Digital Services do not just stay within individual countries; they frequently move from one country to another. As a result, we now have countries around the world that share Multi-Jurisdictional Threats on cyberspace daily due to this type of occurrence. By looking at multiple jurisdictions, we can see how each jurisdiction has chosen to balance their respective Cyber Laws around protect an individuals' Privacy Rights, along with protect the National Security of that nation, along with give Law Enforcement Agencies the tools they need for enforcement and promote Technology Innovation. In addition, doing so creates an environment to develop and find Best Practices, gaps in regulation, and weaknesses in the Cyber Laws of that jurisdiction. Comparing jurisdictions, such as India, the European Union, the United States, and the United Kingdom, allows a Comparative Legal Analysis to support the development of harmonization of Cyber Policy across borders so that we can enhance the capability of enhancing International Cooperation between countries that face Cybersecurity Threats and create a Cybersecurity Legal Framework that is effective and adaptable.

6.2 Comparative Parameters

- **Privacy protection**: Through the binding judicial interpretation of the Charter of Fundamental Rights, the EU provides a constitutional basis for protecting data from both government entities and private companies. This judicial structure ensures that EU Data Protection law has common standards across Member States so that no individual State has discretion to apply lower standards than established by the EU Member State to which the individual belongs. The UK continues with its own strong privacy protections and has separate independent regulatory bodies to continue enforcing those protections. In the United States, Privacy is an unenumerated (but not specifically enumerated) right under the Constitution, therefore, Privacy Rights are not federally established, which leads to more uncontrolled fragmentation, overlaps, and much larger amounts of legislative discretion surrounding Privacy than in the EU or UK context. India has specific laws prohibiting the violation of an individual's right to Privacy, but they do not govern the enforcement of those rights, so there is still legal ambiguity and conflict between statutory law and judicial interpretation of the Constitution in India.

- **Surveillance powers:** Executive authority to conduct surveillance in both the United States and India is often due to national security concerns or countering acts of terrorism and therefore has been given significant latitude. There are oversight mechanisms, however, their transparency and proportionality is quite limited. The European Union regulates surveillance through judicial authorization and necessity and proportionality principles, which creates a situation where state surveillance is more the exception rather than a regular occurrence. The United Kingdom lies between these extremes; the ability to conduct surveillance is permitted, but has been established with appropriate parliamentary and judicial checks.

- **Enforcement mechanisms:** Due to its advanced infrastructure, technical capability, and international reach. In the UK, strong enforcement effectiveness is maintained through specialization in enforcement of their relevant legislation combined with competent judicial authorities. India tends to have a limited preventative enforcement approach, mostly engaging reactively to the enforcement of their legislation. Limitations on India's ability to enforce its legislation stem from a lack of technical capabilities, adequate training, and jurisdictional barriers.
- **Cross-border jurisdiction:** The European Union is the leader in cross border cyber-Governance, primarily through Harmonization and the Export of Regulation (GDPR). The United States exercises Extraterritorial Jurisdiction when it comes to Cybersecurity, but typically does so Unilaterally. The United Kingdom relies on International Cooperation Mechanisms to deliver Cross-Border Cyber Governance. Conversely, India has not yet established a Global Influence for Cyber Governance beyond Bilateral Agreements and Mutual Legal Assistance Treaties (MLAT's) and is, as a result, limited in its ability to influence Global Cyber Governance.
- **Primary cyber law:** Cyber law constitutes the principal legal framework for all cyber-related activity, cybercrime, and e-commerce in a particular jurisdiction or territory. For instance, in India, this is provided by the Information Technology Act, which represents a general guideline for managing cyber activity but is typically a low to moderate level of comprehensiveness. In contrast, regions such as Europe, North America, and the United Kingdom have developed more robust and systematic legislative frameworks that address emerging cybercrime threats in greater detail. The degree of sophistication and comprehensiveness associated with each jurisdiction's primary cyber legislation indicates how well that jurisdiction has kept up to date with the technological progressions within their own country and the ability to create consistent servicing of all components of cybercrime via prosecution and regulatory agency implementations. Conversely, jurisdictions that have non-cohesive or outdated frameworks are frequently

challenged in prosecuting and enforcing their respective cybercrime legislation. Therefore, primary cyber law represents the ultimate stage of governmental sophistication or maturity regarding cyber law governance.

- **Data Protection Law:** The laws surrounding the protection of data dictate the policies that both the governments and private organizations are required to have regarding the usage of personal information. The EU sets the bar by providing the greatest amount of protection, making it an established, substantive right to be protected by law through its comprehensive approach to regulation (the GDPR). The UK follows this same model through its laws, while the USA uses a sector-based approach to provide a moderate level of protection without the establishment of a single federal law. India's data protection framework is still developing with respect to providing necessary individual rights in light of state exemptions; this parameter will demonstrate the level to which a country has made a commitment to ensure that people's personal data is protected in the modern world. Increased strength in the area of data protection leads to increased levels of public confidence and accountability.
- **Judicial Oversight:** Judicial oversight is about how courts authorize and review surveillance and cyber enforcement actions. Strong judicial oversight exists in Europe and the United Kingdom which provides a significant barrier against the excesses of the executive branch. In the United States there is some level of oversight, but the transparency of that oversight is usually limited. In India the judicial oversight of cyber enforcement actions is moderate and while courts play a corrective function, it does not prevent misconduct. This judicial oversight parameter also demonstrates the strength of the rule of law in cyberspace. Accountability in cyberspace is enhanced by effective judicial oversight. Increased risk of abuse of cyber powers due to less oversight.
- **Cybercrime Coverage:** The extent to which a nation's laws define and punish cybercriminal behaviour is indicated by the Cybercrime Coverage Scores of each nation. The European Union (EU) has the broadest Cybercrime Coverage Score due to the

harmonized nature of EU legislation in this area. The United Kingdom (UK) has also provided strong legal coverage for cybercrime via specific laws. The United States of America (USA) and India both provide moderate levels of Cybercrime Coverage via laws that do not comprehensively cover many of the new forms of cybercrime that have developed in recent years. The Cybercrime Coverage Score also indicates how well the legislatures of each nation have responded to the developing risks associated with cybercrime. Strong coverage indicates more effective prosecution opportunities, while weak coverage indicates less opportunity for deterrence and enforcement of penalties against those engaged in cybercrime.

- **Intermediary Liability:** The legal accountability of intermediaries for unlawful acts through intermediaries and/or services ("Intermediary liability") is highly regulated within the EU. In the UK, intermediaries are under a duty to actively ensure compliance with the law, but balance this with safeguards against arbitrary loss of account. The USA has adopted a model of limited liability for intermediaries that supports the concept of intermediaries as vehicles for freedom of expression. India adopts a moderate liability position on intermediaries with the added benefit of 'conditional safe harbor' protections. Each of these factors demonstrates how each nation regulates its digital platforms, influencing the levels of free expression, innovation, and safety on the Internet.

- **Cross-Border Cooperation:** State-to-state cooperation in addressing transnational criminal activity through the use of methods and practices to facilitate recognition and enforcement across jurisdictions. The European Union (EU) provides leadership to this area of governance with respect to EU Member States through coordinated regulations and internal collaboration among Member States. The United States (U.S.) maintains a degree of extra-territorial jurisdiction but has a tendency to act alone. The United Kingdom (UK) utilizes international relationships to provide for these co-operative efforts. Countries with strong enforcement capabilities have the practical ability to enforce their Cyber Crime Laws. The EU, U.S. and UK all provide for strong

enforcement through developed infrastructure and technology expertise. India is continuing to develop its enforcement capabilities and is primarily reactive in its capabilities. This indicator serves to demonstrate the disparity that exists between the legal framework provided for Cyber Crime and the reality of implementation. Strong enforcement provides deterring impacts and encourages compliance with Cyber Laws. Weak enforcement negatively impacts the effectiveness of even the best drafted Cyber Laws. Institutional co-ordination also plays an important role in establishing effective enforcement of Cyber Crime Laws. This area is indicative of the level of global convergence toward cyber governance and the necessity for effective co-operation to combat cross-border cyber threats.

- **Technological Adaptability:** The term adaptability refers to the extent and speed that your cyber laws change and develop as new technologies are invented and developed in order to meet your countries' growing use of the internet. In this way, the European Union demonstrates a high degree of adaptability through continuous regulatory changes and updates while the USA and the UK demonstrate a moderate degree of adaptability through sectoral and judicial legislation but have also shown some capacity for adaptation. India's ability to adapt is improving but is still considered moderate. This indicator also reflects the level of foresight that exists when developing laws related to Cybersecurity. Adaptive legislation minimizes regulatory gaps while ineffective legislation creates outdated legislative frameworks that limit the effectiveness of cyber laws in enhancing long-term cyber resilience.

- **Balance Between Security and Rights:** This dimension represents the balancing of National Security with Fundamental Rights, where both India and the USA are generally security-based; while the EU generally takes a rights-based view, and the UK would be a hybrid of the two. This dimension also reflects a country's constitutional values and democratic history. An excessive focus on security can limit freedom, whereas an

excessive focus on rights can increase difficulty in enforcement. Therefore, a balance of these two positions can create sustainable Cyber Governance.

- **Penalty Severity:** The degree of strictness of Cybercrime penalties ranges from very strict (European Union) to moderate (India) with both the United States and United Kingdom being strict, with India taking a more moderate route to avoid Criminalizing too many people. Penalties reflect how society views Cyber Crime (punitive vs restorative). The effectiveness of Penalties in deterring cybercriminal behaviour is dependent upon the ability to enforce the penalty effectively. Proportionality continues to be important for achieving Justice in these cases.

- **Institutional Capacity:** The skilled personnel, specialist agencies, and technological infrastructure points to a concept called Institutional Capacity in the EU, UK and USA as having established advanced levels of Institutional Capacity; whereas India is still developing its Institutional Capacity but is steadily making progress in developing its Institutional Capacity. Developing Institutional Capacity shows Administrative Maturity in Cyber Governance. The ability to properly investigate and prosecute crimes can be attributed to strong institutions and developing Institutional Capacity must be addressed by developing economies, as it has a direct correlation to the success of its enforcement efforts.

- **Major Enforcement Challenges Level:** This parameter examines how well cyber laws can be enforced, as illustrated by India and American legal enforcement challenges being mostly due to the size of their respective countries, as well as being fragmented and having numerous jurisdictions. That said, within the UK and EU, where there is a greater level of cooperation, overall enforcement challenges have been found to be moderate. Therefore, this parameter demonstrates that the realities of enforcement capabilities exist in addition to legislative capabilities. Weak law enforcement due to high challenges exists; Thus, improving enforcement capabilities will provide for a stronger cyber law regime.

6.3 Comparative Study: India vs EU vs USA vs UK

India, the European Union, United States, and United Kingdom have very different perspectives towards cyber law; each has their own unique legal philosophies, regulations structure as well as regulatory enforcement capabilities. Each jurisdiction also represents a different model of cyber governance based on its respective constitutionally established values, security interests and levels of technological maturity.

6.3.1 India

The legal framework for cybercrime in India is mainly defined by the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. This framework is focused primarily on providing security to the Indian state through vast surveillance (Monitoring, Interception and data Blocking) powers granted to them under Sections 69, 69A and 69B of the IT Act. Many of the new provisions introduced by the DPDP Act align with contemporary concepts of protecting people's data, such as Consent, Purpose Limitation and Data Minimization, however, the vast number of exemptions created for the Indian Government and the lack of adequate judicial oversight have created limits to the effectiveness of these provisions. The Development of an adequate and effective mechanism for enforcing the law is ongoing and will likely face challenges related to the development of additional capacity and access to the necessary technical expertise, as well as Jurisdictional limitations in cases involving cross-border cybercrime.

6.3.2 European Union (EU)

Cyber Law within the European Union takes a rights-based and harmonized approach to Cyber Law. The General Data Protection Regulation (GDPR) sets forth a clear and strong level of protection for individuals' privacy as a fundamental right, through the introduction of strict compliance and enforcement obligations, independent supervisory authorities, as well as high penalties. The also NIS Directive establishes security requirements and reporting obligations for incidents occurring at both Critical Infrastructure, Digital Services Providers. Physical Surveillance Powers, as established within the EU, have been vetted for proportionality and

duly approved by the CJEU and ECHR. Thus the EU exhibits excellent capacity for enforcement, collaboration in a cross-border transaction and adaptability within the law; setting an international standard for governance of Cyber.

6.3.3 United States (USA)

The union of United States expanding cyber-laws are based on Federal Computer Fraud and Abuse act, along with several security measures such as USA PATRIOT. While there are some advantages to having the USA create a cyber-law system that prioritizes national security and law enforcement efficiency; there is some disadvantages with the amount of governmental oversight/monitoring available to law enforcement and government agencies versus the low amount of privacy protections regulated by US Laws to protect personal information... The USA has a well-developed technological and institutional enforcement system, however; without having fully comprehensive data protection regulated by Federal Laws, will be inconsistently regulated by US State laws regarding the privacy protections of each state, and therefore will create a patchwork of inconsistent regulation in place; in addition, the USA is able to enforce US laws globally through extraterritorial Jurisdiction. This has created a great deal of tension in the area of international co-operation, and has affected US relationships with other countries.

6.3.4 United Kingdom (UK)

The United Kingdom has a balanced regulatory framework that allows it to exist between the United States and the European Union. The Computer Misuse Act 1990 applies to cybercrime, while a more traditional approach to the protection of individual data is still governed by the Data Protection Act, which retains the fundamental principles of the General Data Protection Regulation ("GDPR") even after the departure of the United Kingdom from the EU (Brexit). Consequently, there are well-established enforcement agencies and significant judicial oversight of all cybercrime and surveillance, ensuring that they are conducted with proper oversight. The United Kingdom fully appreciates that national security

may require more extensive surveillance, but these powers are subjected to reasonable use through the utilization of strict proportionality and review processes. There is

moderate to strong cross-border cooperation between countries, and the UK also shows a willingness to legally adapt to rapidly changing circumstances in the field of cybercrime investigations across international borders.

6.4 Comparative Tables & Models:

There are significant differences between how each country's legal philosophy, regulation structure and ability to enforce laws will provide a basis to respond to cybercrime and the laws that govern data protection. The Cyber laws of India are primarily derived from the Information Technology Act, 2000. The Digital Personal Data Protection Act, 2023 currently being developed also emphasises increased powers of security and surveillance as well as continuing development of judicial oversight; Indicating the fact that the legal framework of India remains in a constant state of evolution and evolving nature. Therefore, there is considerable uncertainty relating to the content of India's laws. Comparatively comparing different countries cybercrime legal frameworks allows for an easier understanding of how cybercrime laws (on a legislative, institutional, and enforceable basis) operate in relation to each other, with respect to the connection between India and other jurisdictions (EU, USA, and UK). Therefore, it is evident that each jurisdiction has devised a unique approach to address cyber threats while addressing obligations of supporting both the technological growth of the jurisdiction, as well as the need for security and privacy.

Primary Cyber Law in India is Moderate in terms of Implementation, as it is based primarily on the IT Act 2000-Legislation. While the IT Act is the Foundation of Cyber Law in India, it is an older and less updated source than other jurisdictions that have created Comprehensive, Sectoral Approaches to Cybersecurity Laws (EU, USA, and UK). The European Union provides Strong Data Protection through the GDPR, which considers Data Protection a fundamental human right. While the UK offers Strong Data Protection for individuals through

its own GDPR. At this time, both India and the US are both considered to have Moderate Levels of Data Protection, and India is in the process of creating an Evolving Framework of Data Protection with a sector-based approach; in the US, Sector-based Data Protection is fragmented .The European Union and United Kingdom have a strong legal framework of privacy protection and implementing very strong enforcement mechanisms to maintain such privacy protections. Comparatively speaking, India and the United States have moderate levels of privacy based on the balancing of privacy rights with the coercive authority of their respective Executives, as well as national security.With respect to the respective nation's philosophies of law in relation to surveillance, there are significant differences in the scope and degree of authority exercised by the respective nation's governments.

Both India and the United States grant significant authority to their respective Executives with respect to the conduct of surveillance in support of their national security, including counterterrorism, whereas the European Union has a balanced, legally sufficient, and accountable framework, to include proportionality, proportionality safeguards, and judicial review processes. Similarly, the United Kingdom exceptionally possesses very expansive Executive Surveillance Power with significant accountability for abuses of that power.

Judicial checking and oversight, the European Union and United Kingdom organisationally create sophisticated means to oversight and restrict government use of Executives' power; while India provides reasonable judicial review capabilities, generally after the fact. On the other hand, the United States has not effectively developed processes to enable constructive scrutiny of the manner and extent to which it utilises surveillance mechanisms. The EU has a significant amount of cybercrime protection through a variety of harmonised legal instruments. There is also a significant amount of cybercrime protection offered in the UK. The level of cybercrime

protection offered to both India and the United States is moderate; however, there are still areas in which they are not able to adequately address new and/or more complex types of cybercrime.

Each of the governments enacts laws regarding intermediary liability and holds digital platforms responsible for both the content that is published on their platform and for what happens to the content once it is published. The EU's laws state that digital platforms need to take on a significant amount of accountability for the content that is being published on their platform. The UK and India have Moderate Liability standards with conditional protections for digital platforms, and the United States uses a very limited liability approach primarily for the purpose of fostering innovation and freedom for digital platforms. The enforcement capabilities of the EU, the United States and the UK are strong because these countries have advanced institutions that employ skilled people, as well as the level of technological infrastructure that supports these institutions. In contrast, India's enforcement strength is Moderate because the country is still developing its institutional capabilities and has technical limitations. In the context of transnational cooperation, the European Union is characterised by an efficacious system of harmonisation, high levels of co-ordination among its member states and the operation of a centralised governance mechanism. Conversely, the USA and UK operate at a more modest level of co-ordination and perform in a cooperative manner on a more ad hoc basis through bilateral or multilateral agreements. While India continues to have a somewhat limited position in relation to transnational cooperation and primarily relies upon bilateral agreements and Mutual Legal Assistance Treaties to engage in transnational cooperation.

The European Union has been highly flexible with respect to its regulations in relation to technology as the technological landscape evolves. As a result, the European Union is at the forefront of the development of technology regulations. Conversely, the USA, UK, and India, although they are somewhat flexible regarding technology, typically respond to new legislative

developments at a slower pace than the EU.Security and civil liberties define how jurisdictions interact with one another and how a government in that jurisdiction provides services to its citizens. For example, the USA and India have a national security-oriented model for state and local police departments that incorporates secret intelligence activities as well as foreign intelligence activities; in contrast, the European Union employs a civil rights-based approach to its law enforcement, security and intelligence functions. The UK employs both a national security and civil rights model, positioning itself in between the EU and both the USA and India.Penalties are designed by the EU to be extremely high so as to act as a deterrent, whereas both the USA and UK have a more moderate penalty structure with penalties ranging from medium to high. In contrast, India has a more moderate penalty system focused on proportionality.The EU, USA and UK have developed higher levels of institutional capacity, with the institutions benefiting from a higher level of expertise and agency specific to their institutions; in India, the capacity is still being developed, however there is ongoing development.Third, the enforcement challenges facing the USA and India are still at a major level because of fragmentation, scale and jurisdiction problems, while the EU and the UK have moderate institutional maturity and coordination thereby experiencing reduced enforcement challenges.

The Table displays that in advanced jurisdictions, Rights Protection, Enforcement Capacity, and Institutional Strength are much more effectively developed than in developing nations or jurisdictions; however, developing countries face similar challenges in finding a proper balance between the obligation of Cybersecurity and Civil Liberties within the Transnational Digital Scenario.On the one hand, the European Union has an established Rights-based and Harmonized Model; through the combined effect of the General Data Protection Regulation (GDPR) and the NIS Directive, both create a strong Privacy Protection environment, with high Intermediary and Judicial Obligations on an International Basis, along with Severe Penalties to

ensure compliance and set an International Benchmark for Data Governance, It Includes the Following: a) The GDPR, b) The NIS Directive, c) The right to Privacy, d) Judicial Oversight, e) Penalties for non-compliance.

On the other hand, the United States of America has a Non- Harmonized and Disparate Jurisdictional Approach for data privacy and protection within an increasingly globalized economy. The United States primarily regulates data Privacy and Protection through Statutes that are specific to the type of Information, such as the Computer Fraud and Abuse Act and The USA PATRIOT Act, which give priority to National Security and Law Enforcement and Facilitate surveillance and the ability to monitor activities with Limited Privacy Protection. In Table 6.1, Comparative analysis of UK,USA , Europe and India.

Aspects	India	European Union(EU)	United State	United Kingdom(UK)
Primary cyber-Law	Moderate	Strong	Strong	Strong
Data protection Law	Moderate	Very Strong	Moderate	Strong
Privacy Protection	Moderate	Strong	Moderate	Strong
Surveillance Powers	High	Balanced	High	High
Judicial Oversight	Moderate	Strong	Limited	Strong
Cybercrime Coverage	Moderate	Comprehensive	Moderate	Strong
Intermediary liability	Moderate	Strict/strong	Limited	Moderate
Enforcement Strength	Moderate	Strong	Strong	Strong
Cross border Cooperation	Limited	Strong	Moderate	Moderate

Technological adaptability	Moderate	High	Moderate	Moderate
Balance between security and rights	Security oriented	Rights oriented	Security Oriented	Balanced
Penalty Severity	Moderate	Very High	High	High
Institutional capacity	Developing	Advanced	Advanced	Advanced
Major Enforcement challenges Level	High	Moderate	High	Moderate

Table 6. 1 Comparative analysis of USA, UK, India and Europe

By taking a middle position between offence-specific statutes governing specific types of cybercrimes as outlined within their Computer Misuse Act along with having a plethora of courts with well-developed judicial processes that allows them to enforce very strong laws regarding these crimes. They also balance these two areas with multiple views on civil liberties versus national security priorities, which have also varying degrees of impact with respect to enforcement and compliance as a result of jurisdictional differences related to their technological abilities to create new laws, the way they establish laws regarding enforcement versus compliance and their maturity with respect to the legal framework used to govern cybercrime. The comparison demonstrates that there exists a state of tension throughout the global community between the two areas related to cybersecurity and civil liberties because advanced regulatory frameworks will make enforcement stronger and provide greater

accountability, but such frameworks must continue to change to meet the rapid pace of technological change caused by transnational cyber threats to maintain a balance of security and fundamental rights.

A deeper examination of cyber law governing how India, the European Union, the United States and the United Kingdom view cyber law in a large scope reveals that each of these jurisdictions view cyberspace as a regulated space in different ways based on their respective national legislatures and regulatory philosophies, and political priorities.

The way that digital rights are treated in constitutional law is another important distinction. In Europe, the right to privacy and data protection is clearly established as a basic human right in the EU Charter, and has been subsequently interpreted by the European Court of Justice, which creates uniform enforcement of this right to all EU Member States with limited ability for individual Member States to exercise discretion regarding enforcement. While the UK, as a former member of the EU, maintains similar constitutional values through domestic legislation and established regulatory bodies, the US and India derive much of their privacy protection through judicial interpretation rather than constitutional or statutory law, thus allowing for greater discretion by the legislature and executive branches in regulating cyber activities.

Securing a balance is called a 'security/rights trade-off' and it is significant. In both India and US cyber governance models the primary driver is Security. Both countries priorities law enforcement and national security. This results in a quick response to cyber threats and terrorism; however, it significantly increases the power of surveillance and decreases the amount of transparency. The European Union has an integrated rights first approach towards surveillance. Surveillance is viewed as an exception and not the norm. Hence it has stringent tests of 'necessity' and 'proportionality' placed on the use of surveillance. The United Kingdom occupies a Hybrid position. Countries with Long-Standing Cyber Crime Enforcement Policy Structures/Agencies in the EU, USA and UK have a proven track record of supporting advanced technology and skilled investigations, enabling proactive, coordinated attack responses and cross-border cyber-crime prevention through engagement with law enforcement across nations.

In addition, the cybersecurity ecosystem of India is emerging and growing but currently lacks sufficient capacities due to its modest base of available capacity, lack of capacity/knowledge related to multiple aspects of cybersecurity and protracted court systems that result in late and/or inadequate/unsuccessful investigation and prosecution of modern day global cyber crime threats.

There are notable distinctions in the ability of regulators to adapt to quickly changing technologies. The EU appears to have a strong ability to maintain a high level of adaptability through continuous updates of their regulations and a proactive approach to developing digital policies (such as allowing for growth), as well as having the capacity to keep pace with rapidly growing innovative technologies; for example, artificial intelligence and large data analytics technologies. The US and the UK take a different approach to regulating the digital world by utilising a segment-based regulatory and judicial interpretation; this has provided them with moderate ability to adapt to the technological marketplace. India's ability to adapt and be able to respond to this evolving technology space has been improved due to their recent legislative initiatives, but further work is needed to promote the usage of drafting legislation that is neutral to technological changes and provides for more flexibility and adaptability to the marketplace.

In a global context, Europe has a significant influence on the evolution of global cyber governance. In addition, while the US also has an extraterritorial reach, with particular emphasis on national security and financial regulation issues, they have been perceived to create tensions with other jurisdictions internationally. The UK has primarily been focused on multilateral and bilateral agreements for cooperation, and India primarily relies on mutual legal assistance treaties to establish cyber governance frameworks, which currently limits their ability to establish global cyber governance norms.

Across the globe, there are many different ways to protect against cyber threats. Although the four different jurisdictions outlined in this study each focus on similar types of cyber threat protection, they do so based on different legal philosophies and governing structures. The European Union has developed a rights-based, harmonised approach, while the United States continues to emphasise enforcement through a security-focused framework.

Whereas, the United Kingdom has provided a balanced combination of both approaches and India has developed a transitional legal and governance structure in which there is an attempt to balance the security needs inherent in the emergence and expansion of the digital environment, with newly developed digital rights. All four jurisdictions illustrate the necessity for improved international co-operation and more inclusive, technology-neutral laws associated with the enforcement of digital rights to protect against the emergence of global cyber vulnerabilities that will impact all jurisdictions across the globe.

6.5 Strengths and Weaknesses

By assessing strengths and weaknesses of Cyber Law, we provide a structured view of how effective, limited, and broadly used legal frameworks are for combatting Cyber Crime, protecting Privacy, providing Enforcement, and dealing with Technology Change(Slauson). Strengths of a Cyber Law may include strong government-supported and/or enforced protection, clearly defined rules and regulations, strong institutional support, or effective Enforcement mechanisms. Weaknesses may include gaps in legislation, inappropriate levels of or Surrendering Authority, and inadequate Judicial review, etc. The purpose of Comparative Analysis of Strengths and Weaknesses is to understand how Jurisdictions have become more or less Successful with respect to certain Topics, while also providing us with an understanding of whether or not there is a Need for Cyber Law Reform. Cyber Law Reform is intended to create a more Balanced, Rights Protecting, and Secure Cyber World.

6.5.1 India

Strengths

- Surveillance powers provide national security and support investigations of cyber-terrorism events.
- Penalties for crimes can be administered in proportion to the offense and also increase the likelihood of preventing conduct from being over-criminalized.
- The Government of India is expanding the number of agencies with the ability to conduct investigations of cyber-criminal activity by establishing CERT-In, NCIIPC, and Cyber Crime Cells, allowing the Government of India to investigate cyber-criminals more rapidly and effectively.
- A security-based framework enables the Government of India to respond quickly and efficiently to threats associated with cybercrime.

Weaknesses:

- The principal cyber law (IT Act, 2000) is moderately organized but does not sufficiently address modern cybercrime risks.
- In user rights, the modest coverage of privacy and protection of data has resulted in several gaps.
- Investigating and prosecuting cross-border cybercrime has been severely hampered by poor international collaboration.
- The issues in this effective enforcement of cybercrime laws exist due to the judicial delays and partial technical expertise.

6.5.2 European Union (EU)

Strengths

- To confirm strong personal data safeguards by using robust data protection law (GDPR).
- Standard legal instruments for addressing cybercrime.
- A rigorous standard of judicial scrutiny protects everyone's civil liberties.
- A high degree of technical adaptability allows for quick and effective responses to emerging issues in cybercrime.
- A balanced encouraging reaction to both fundamental rights and attempts to enforce them has been produced by placing a strong focus on the preservation of rights when pursuing criminals.
- Among member states, build the very strong cross-broader cooperation.

Weaknesses

- Small and medium businesses may be burdened by extremely severe penalties.

- Multiple regulatory levels result in complex compliance requirements.
- Moderate enforcement challenges, especially due to coordination across jurisdictions.
- The implementation of balanced surveillance powers could slow down an urgent response to national security threats.

6.5.3 United States (USA)

Strengths

- Clearly defined cyber laws at the national level that include significant sector-specific regulations.
- Advanced institutional capacity supported by agencies like FBI, DHS, and CISA.
- Strong enforcement strength, particularly in financial and infrastructure protection.
- High penalty severity, acting as a deterrent against cybercrime.
- Robust monitoring capabilities assisting intelligence-driven cyber operations.

Weaknesses

- Nationally, there are limited judicial checks & balance on public authorities monitoring citizens
- Although there is a medium data protection framework, there is no comprehensive federal data protection regime
- The emphasis on national security may impact individual privacy rights negatively
- Limited liability for intermediaries results in minimum accountability for digital content providers
- The inability to effectively enforce laws due to jurisdictional disparity between states is a significant challenge.

6.5.4 United Kingdom (UK)

Strengths

- Robust core cyber laws with well-defined enforcement procedures.
- Strong privacy and data protection aligned with UK GDPR.
- Strong judicial oversight, ensuring accountability of surveillance actions.
- Advanced institutional capacity with agencies like NCSC and ICO.
- Between balanced approach to the individual rights and security.

Weaknesses

- Civil Liberty concerns arise from high levels of surveillance power.
- Cross-border cooperation is moderate, especially since the United Kingdom left the EU (Brexit).
- Intermediary liability is moderate and creates uncertainty for various platforms
- Technology is changing at a relatively moderate rate and requires an equally quick updating of regulations.
- Enforcement problems are moderate, in particular where there are international complexities surrounding cases.

6.6 Comparative Summary:

The comparative review of cybersecurity legislation frameworks throughout the United States, United Kingdom, European Union, and India shows significant differences due to variations in constitutional values, government priorities for national security, and levels of developed institutions. The cybersecurity legislation of India is primarily focused on providing for a strong national security response capability to cyber threats; however, it lacks adequate protection of the right to privacy, broad coverage of cybercrime, and the ability to impose criminal jurisdiction on a transnational level. Conversely, the European Union is the "Most Rights Based" and harmonized model of cyber governance in the World. As an advanced, well-structured and rapidly growing system for data protection and enforcement there are effective methods for international cooperation, judicial oversight. However, the complicated system of compliance combined with stiff penalties associated with non-compliance to this legislation could be overwhelming for smaller organisations. The law enforcement power and technological capabilities in the USA may arguably be the highest performing in the world due to the extensive amount of surveillance capabilities and the highly-skilled enforcement agencies that provide assistance to these enforcement activities. Conversely, due to the fragmentation of the privacy laws in the United States, there is no single comprehensive national law which defines how personal data should be used, creating many different types of privacy protections across the nation.

While the overall strength of law enforcement, judiciary, and regulatory systems in the United Kingdom are in fairly equal balance, there could be new challenges resulting from Brexit, such as developing a unified cyber legal framework with other nations. By examining the current state of cyber law, we can understand better how the on-going struggle exists between the need to protect and maintain national security interests and the protection of

individual civil liberties. Cyber legal frameworks need to continue adapting to the rapidly evolving global landscape through continued cooperation internationally to ensure that protections are maintained for individuals

CHAPTER 7

FINDINGS, OPPORTUNITIES & PROPOSED FRAMEWORK

This section includes a narrowing of the scope at the end of the research analysis on cybercrime, including re-assessing the research question from this chapter. The legal and legislative suggestions provided were created to protect people's access to their fundamental human rights while increasing enforcement mechanisms against cybercrime activity. Finally, we explore additional areas requiring further study due to rapid growth in the areas of cyber security and cybersecurity law.

7.1 Key Findings

The research findings indicate that cybercrime is traditionally viewed as a serious global threat that threatens an individual’s value to society through their privacy, as well as the legal system; however, cybercrime has been viewed as a threat to nation states and sovereignty, as it infringes upon existing country’s laws and therefore provides a degree of legal insecurity within a country or region. The Indian Constitution does not guarantee a person’s right to privacy; however, the Indian cyber laws tend to support security as the driving force behind any government activity. The laws create a conflict in that while the United States Government promotes industry efficiency.

British Government has adopted an even standards-based approach through the use of a strong interface of judicial oversight that enables balanced use of security and privacy, and the European Union has developed a legal structure designed to maintain a broad-based level of rights addressing a person's privacy. Aside from the fact that there is a discrepancy between how fast technology has developed compared to how slow regulation has been to keep up with new technologies, the same can be said when considering how AI may affect Law Enforcement & Cyber Security. There are also many things we learned and saw from the results of our research. The findings show that there is an urgent need for legislators to create flexible, technology-neutral and human rights-respecting legal frameworks that maintain the Constitutionally protected rights of individuals in light of the rapidly changing nature of Cyberspace.

7.2 Legal Challenges Identified

The report identifies the following major areas of law that affect the areas of privacy, national security and cybercrime regulation

- **Legal Uncertainty in Cyberspace:** Cybercrimes occur in many different countries (in terms of due process) therefore it may be difficult to determine what jurisdiction applies to any specific case, including which courts are able to hear cases involving cybercrime and what laws may be enforced by those courts. Jurisdictions are often disputed and have often been delayed by the fact that current standards for determining territorial jurisdiction do not work for the internet or cyberspace.
- **Judicial Oversight of Security Agencies is Insufficient:** The surveillance and interception powers of most Executive (i.e. Police and Military) Security Agencies do not include any transparency through regular review and monitoring or prior authorization from the Courts. This allows for the potential for abuse, and diminishes the protections provided by the Constitution.
- **Statutory Text (General):** "National security," "public order," and "sovereignty" appear frequently as ambiguous terms within cyber security laws, permitting an area for unrestricted execution of the law based on interpretations made by law enforcement officials and/or courts.
- **Insufficient Oversight of "Emerging Technology":** Law enforcement agencies utilise a range of technologies (e.g. Artificial Intelligence, Machine Learning, Facial Recognition, and Big Data) for cyber safety and surveillance. However, the present legal framework offers no mechanisms for holding agencies accountable; for supporting transparent decision-making processes based on the output produced by algorithms; or for creating any liability for the algorithmic nature of decisions made.

- **Insufficient Protection of Digital Privacy:** Digital privacy is not adequately protected by statutes, which allow state agencies and other governmental agencies to circumvent data protection duties and diminish the privacy, autonomy, and self-determination rights of individuals.
- **Low Conviction Rates in Cybercrime Cases:** The very low rates of conviction on cybercrimes is caused by delays in the judicial process, the fact that police investigators and judicial officers are not trained in the technical knowledge necessary to investigate and charge cybercriminals, lack of evidence and lack of forensic capabilities to perform evidence collection, and also inadequate evidence-gathering capacity in most jurisdictions.
- **Lack of Clear Data Localization Standards:** There is much confusion with regards to the rules related to data localization and therefore creates a challenge to both law enforcement agencies and private companies trying to enforce their laws as well as comply with these requirements when accessing data from outside their country.
- **Overdependence on Executive Rule-Making**: In over reliance on Delegated Legislation and Executive Rules diminishes parliamentary control on Cyber Governance, thereby diminishing democratic accountability for actions taken.
- **Fragmented Cyber Incident Reporting Mechanisms:** Due to the absence of a comprehensive and mandatory Cyber Incident Reporting Framework, there is a lack of information collected when a cyber event occurs, thus leading to a low response rate and a lack of timely reporting and effective analysis of cyber incidents. **Insufficient protection exists for whistleblowers and Ethical Hackers:** The lack of legal safeguards for whistleblowers and ethical security researchers discourages responsible disclosure of cyber vulnerabilities.

- **Limitations of Cross-Border Enforcement:** Mutual Legal Assistance Treaties (MLATs) take considerable time, are outdated and bureaucratic and are not suitable for cybercrime investigations carried out in real-time
- **Lack of Specialized Cyber Courts and Expertise**: No Cyber-Specific Courts and Expertise Courts of general jurisdiction do not usually possess the expertise required to deal with complex types of cyber evidence, resulting in inconsistent outcomes and protracted legal proceedings
- **Digital Policing's Ethical Questions:** Using mass data collection, predictive policing and profiling of individuals raises ethical issues about discrimination, proportionality and misuse of personal information.
- **Lack of Technology-Neutral Definitions:** Cyber laws have been developed for the current state of technology, without accounting for future changes seen in technology such as artificial intelligence, blockchain, quantum computing and the Metaverse. The result is that all of these rapidly-evolving technologies create a blind spot in regulatory terms, thus resulting in no regulations or totally inadequate regulations in these areas.
- **Decentralised Institutions for Cyber Governance:** Numerous government agencies have jurisdiction and oversight over similar areas, such as anti-cybercrime, surveillance, data protection and national security. Therefore, absent interagency co-operation, authorities may duplicate one another and create confusion around the direction of the regulatory and enforcement functions.
- **Limited Accountability for Intermediaries & Online Service Providers:** Intermediaries play a vital role by providing users with the ability to collect and share information with each other, moderate content and protect against cyberattacks. However, the insurance liability structure established by governments creates problems for intermediaries in terms of how to position

themselves legally. There are far too many examples of laws that create an extremely large amount of flexibility in terms of what constitutes "intermediaries" while simultaneously creating a system of inequity with respect to intermediary accountability and complicating enforcement of cyber-related offences.

- **Challenges to Evidence for Digital Forensics**: There are several problems related to evidence in digital forensics, including that digital data can be easily modified and is difficult for many people to interpret due to its physical properties. For courts, issues surrounding the evidence include whether or not (1) the digital evidence is authentic, (2) there is a proper chain of custody of the digital evidence, (3) the digital evidence will ultimately be accepted by a court, and (4) the digital evidence will ultimately lead to an accurate and reliable forensic analysis of the evidence. As a result of these challenges, there have been delays and acquittals in prosecuting cybercrime.
- **Disproportionate Effects of Mass Surveillance:** Mass surveillance, predictive policing and data analysis, have resulted in an extraordinary impact on individuals' ability to speak freely, associate with others freely and remain anonymous when engaging in activities in digital areas. The inability to protect freedom of speech and association has created huge uncertainties regarding constitutional rights and democratic freedoms.
- **Inadequate Legal Safeguards Against Algorithmic Discrimination:** AI-driven cybersecurity-tools, law enforcement tools, etc., are likely to rely on existing biases within the data and the algorithms. There are currently no definitive legal protections against the use of algorithmic discrimination, which jeopardizes individuals' rights to equal protection and due process.
- **Weak International Norms on Cyber Warfare and Cyber Terrorism:** There is no single universally binding international legal framework in existence today that defines the responsibilities for states and individuals when conducting cyber-

attacks. As a result, both states and individual actors currently have only the restraints of international law to protect their interests when conducting cyber-attacks.

- **Limited Victim-Centric Legal Remedies:** Cyber law frameworks primarily focus on punishment and security, often neglecting victim compensation, psychological harm, reputational damage, and data restoration remedies for cybercrime victims.
- **Poor Public Awareness and Digital Legal Literacy:** Lack of awareness among citizens regarding cyber laws, digital rights, and reporting mechanisms results in under-reporting of cybercrime and reduced effectiveness of enforcement mechanisms.

7.3 Opportunities for Reform

- **Development of Technology-Neutral Cyber Legislation:** By drafting cyber laws using technology-neutral language, the potential for reforming cyber law is very high. Technology-neutral drafting makes the laws flexible enough to adapt to future innovations and will also prevent cyber laws from becoming obsolete because of changes in technology. Through the use of technology-neutral language, cyber laws can respond to changes in cyber threats over time including artificial intelligence, quantum computing, blockchain and metaverse-based environments.
- **Improve the Judicial Process:** With mandatory judicial supervision, periodic review of orders obtained by law enforcement, and the issuance of written orders for interception and surveillance, judicial oversight will greatly improve compliance with the Constitution, minimize excessive use of authority by the executive branch, and establish greater public confidence in national security programs
- **Increase the Number of Cybercrime Units and Institutions with Cybercrime Expertise:** The establishment of specialized cybercrime units, cyber forensic laboratories, and ongoing professional development for judges, prosecutors, and investigators is an excellent opportunity to improve the quality of cybercrime investigations, success rates for prosecutions, and consistency among courts on cybercrime cases.
- **Create a Centralized National Cybercrime Coordination Agency:** A Centralized Cyber Crime Coordination Agency integrates Law Enforcement, Intelligence Agencies, Regulators, and Private Sector Coordination facilitating Coordination among all while eliminating redundant and fragmented coordination.

- **Provide Government Incentives to support Privacy-Enhancing Technologies (PETs):** By having a law that supports Individual Rights along with owning their Personal Data, the availability of PETs (i.e., Encryption, Anonymization and Secure Computation) increases Security and Individual Rights.
- **Integrating Ethical-by-Design Cyber Laws:** As part of Cybersecurity and Monitoring Policy provides Cybersecurity with a Framework for Proactively Identifying and Mitigating: Potential Discriminatory Actions - Misuse of Personal Data, and Violation of Individual Rights (i.e., Freedom of Expression).
- **Using Explainable AI as an Oversight Tool for Law Enforcement:** AI-based systems (e.g., Cybersecurity Systems and Criminal Justice Systems) must have mandated requirements imposed which will ensure Transparency, Accountability, and Fairness in the Automated Decision-Making Process (as directed by an AI System). Such mandated requirements can assist Government Agencies and Private Corporations in ensuring a Proper Oversight mechanism exists for AI-based systems.
- **Increasing the Government(s) Governance of Personal Data Protection:** Increasing government(s) Independent Data Protection Authority and Centre/Office will strengthen Compliance by Private Sector Companies, Heighten Institutional Accountability, and Build Public Confidence in Digital Governance Systems.
- **Public-Private Partnerships in Cybersecurity:** Cybersecurity continues to create an environment for an opportunity for Structured Collaboration between Government, Technology Corporations, Financial Institutions, Civil Society, and Intelligence Agencies to share data on Cyber Countermeasures (and Threats), to establish Best Practices, and to Improve the Resilience and Strength of Nation States against Cyber Threat.

- **Establishing Cybercrime Courts with Specialized Judges:** Dedicated cybercrime court systems can expedite the judicial process because the judges assigned to these courts will have specialised training in cybercrime adjudication and will therefore have the requisite knowledge to make informed legal decisions regarding the issues associated with cyber evidence and other technical matters related to the prosecution and defence of cybercriminals.
- **Creation of Modern Methods and Processes for Collecting Digital Evidence:** Developing a process for the authenticating and collection/proof of digital evidence, including identifying what constitutes digital evidence, how this digital evidence is collected, stored, preserved and used is likely to provide a stronger foundation for successful prosecution and increase confidence in the evidence being presented to the court.
- **Implement Victim-Centered Cyber Justice:** Victim-Centered Cyber Crime Law can evolve from being strictly punitive in nature to providing rehabilitative options, including compensating victims; restoring lost digital property through reparative psychological support; providing prompt and equitable access to a platform through which to file grievances regarding all aspects of cybercrime.
- **Enhance Cross-Border Cyber Investigation Mechanisms:** The ability to create and implement alternative mechanisms (replacing outdated MLATs with real-time data sharing) as well as developing multi-national arrangements such as Joint Cyber Task Forces, will provide important ways to combat worldwide cybercrime.
- **Regulation of Surveillance through Proportionality Principles:** Proportionality principles are necessary for regulating surveillance lawfully and balancing the need to protect national security against the protection of citizens' fundamental rights. National security can be protected while citizens' rights are

respected through the use of constitutional principles of legality, necessity and proportionality as part of the framework of a surveillance law.

- **Improving Accountability of Digital Intermediaries**: It can occur through the reform and enhancement of the regulations governing the intermediary liability of the digital intermediary to include an equal share of responsibility by the intermediary for the actions of third parties, obligations to provide transparent processes for reporting complaints, and due process rights for both the intermediary and third parties.
- **Expanding awareness of Cyber Law and developing Digital Literacy:** By providing all citizens and governments with public awareness campaigns related to cybercrime against citizens and Digital Cyber Literacy through education programs related to Cyber Law can improve enforcement outcomes through increased reporting rates and improved resilience against cyber crime by citizens.
- **Development of Global Cyber Governance Norms:** Contributing to the development of international law regarding Cyber Warfare, Cyber Terrorism and State Sponsored Cyber Operations is a long-term opportunity to establish binding international norms of conduct that will enhance accountability and stability in cyberspace.

7.4 Policy Recommendations

- **Create a New Cybersecurity and Surveillance Oversight Law:** Legislation regulating the surveillance, interception, retention of data, and AI monitoring should be introduced by the Government of the United States. Legislation should require judicial oversight of all activities and data used by surveillance programs; proportionality tests after the collection or retention of data; and transparency requirements.
- **Create Dedicated Cybercrime Courts:** Establish dedicated courts to hear and decide all Cybercrime cases by Technically Trained Judges to ensure swift resolution and consistency in Cybercrime Jurisprudence
- **Require Compliance with Explainable AI and Accountability Standards:** The AI Systems Utilised by National Security and Law Enforcement should have to comply with a framework of Mandatory Explainability, Bias Assessment, Algorithm Audit, and Human Accountability.
- **Create Mandatory Cyber Impact Assessments:** prior to the activation of new large-scale surveillance, AI-based policing, or National Cybersecurity projects, Cyber Impact Assessments and Human Rights Impact Assessments must be conducted
- **Statutorily Protect Ethical Hackers and Responsible Disclosers:** Establish statutory protections specifically for Ethical Hackers and Responsible Disclosers who report vulnerabilities in good faith.
- **Establish a Unified National Cyber Incident Reporting System:** Create a single, centralized, mandatory, and time-bound Cyber Incident Reporting System to enable improved early detection, coordinated responses, and cyber intelligence sharing.
- **Strengthen Parliamentary Oversight over Cyber Governance:** Parliamentary Committees Need to Be Empowered to Review Cybersecurity Policies, Monitoring

Systems, And AI Implementation to Hold Governments Accountable and Ensure That All That Is Done in The Name of Security Is Done with Democratic Oversight

- **Strengthen Cross-Border Cybercrime Cooperation:** States Need to Revise Their Mutual Legal Assistance Treaty Procedures, And Create New Protocols for Sharing Data in Real Time, and Be Part of a Global Convention to Help All Countries Increase Their Cyber Crime Enforcement Capabilities.
- **Limitations if executive discretion through Statutory safeguards**: There needs to be an Independent Oversight process for Government Exemptions from DATA Protection & Cyber Security Laws. These Statutory Exemptions should only be given out under a strict definition and time limits, and must be reviewed by an Independent Person or Agency.
- **Increased public knowledge and transparency regarding Digital Rights**: There is a need to provide the public with information gathered by the Government regarding Surveillance Frameworks, Reports from Oversight Bodies and Impact Analyses. Public Knowledge Can Aid in Holding the Government Accountable for Whatever Action the Government takes in the Name Of Democracy.
- **Nations should align their National law**: Good International Cybersecurity practices and Data Protection laws. The European Union has created a rights-centric approach which can be utilized as a foundation for developing National Cybersecurity and Data Protection statutes in many nations. Each Nation must also develop Cybersecurity and Data Protection statutes in accordance with their Constitution and at the same time strive for Balancing Privacy with Security.

7.5 Future Scope:

Both cybercrime and digital technologies will grow over time, as will the future of research in these areas. As they develop it will be important for the legal systems and supporting institutions to adapt to this changing landscape. The emerging technologies that will be developed through continued research in these areas include AI/Policing, Quantum Computing, and Blockchain Systems. Additionally, the unique regulatory issues that will arise in relation to Metaverse platforms will require further development of both scholarly and policy-oriented research going forward. Research in the future will likely include the creation of a "Unified International Standard" for Cyber Crime, methods to improve Global Cyber Crime Law Enforcement, and adequate means for the courts to handle the complexity of Digital Evidence. Other research may centre on better defining Cybersecurity Frameworks from a Human Rights perspective and developing Governance Frameworks for the use of AI. The outputs from both of these areas of research will help create an equilibrium between the National Security needs of the Digital Age and the Privacy/Individual Protection Rights of Citizens.

REFERENCES

1. Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., ... & Gangarde, R. (2024). Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. *Engineering Proceedings*, *62*(1), 6.
2. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.
3. Raman, Shiv and Asthana, K. B. (2025). Investigation of cyber crimes in India new issue challenges and strategies, http://hdl.handle.net/10603/664530
4. Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal*, *38*(1), 29.
5. Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks*, *11*(6), 101.
6. Pina, E., Ramos, J., Jorge, H., Váz, P., Silva, J., Wanzeller, C., ... & Martins, P. (2024). Data privacy and ethical considerations in database management. *Journal of Cybersecurity and Privacy*, *4*(3), 494-517.
7. Sousa, S., & Kern, R. (2023). How to keep text private? A systematic review of deep learning methods for privacy-preserving natural language processing. *Artificial Intelligence Review*, *56*(2), 1427-1492.
8. Mishra, Shashya (2023) A Critical Study On Cybercrime With Special Reference To Women In India http://hdl.handle.net/10603/454392
9. Awadallah, A., Eledlebi, K., Zemerly, M. J., Puthal, D., Damiani, E., Taha, K., ... & Yeun, C. Y. (2024). Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities. *IEEE Communications Surveys & Tutorials*, *27*(2), 1008-1052.
10. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804.
11. Phang, K. C., Ng, T. C., Singh, S. K. G., Voo, T. C., & Alvis, W. A. (2025). Navigating Artificial Intelligence in Malaysian healthcare: Research developments, ethical dilemmas, and governance strategies. *Asian Bioethics Review*, *17*(3), 631-665.

12. Park, I., Kim, D., Moon, J., Kim, S., Kang, Y., & Bae, S. (2022). Searching for new technology acceptance model under social context: Analyzing the determinants of acceptance of intelligent information technology in digital transformation and implications for the requisites of digital sustainability. *Sustainability*, *14*(1), 579
13. Iwasaki, M. (2025). Banning ransomware payments: unintended effects on cybersecurity investment and incident reporting. *International Cybersecurity Law Review*, *6*(1), 17-27.
14. Maras, K., Sweiry, A., Villadsen, A., & Fitzsimons, E. (2024). Cyber offending predictors and pathways in middle adolescence: Evidence from the UK Millennium Cohort Study. *Computers in Human Behavior*, *151*, 108011.
15. Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the academy of marketing science*, *50*(6), 1299-1323.
16. Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, *15*(1), 83-106.
17. Al-Surkhi, W. A., & Maqableh, M. (2024). The impact of cybercrime on internet banking adoption. In *Current and Future Trends on Intelligent Technology Adoption: Volume 2* (pp. 231-245). Cham: Springer Nature Switzerland.
18. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.
19. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.
20. Dupont, B., Fortin, F., & Leukfeldt, R. (2024). Broadening our understanding of cybercrime and its evolution. *Journal of Crime and Justice*, *47*(4), 435-439.
21. Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors*, *23*(3), 1151.
22. Velasco, C. (2022, May). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. In *ERA Forum* (Vol. 23, No. 1, pp. 109-126). Berlin/Heidelberg: Springer Berlin Heidelberg.

23. Nwafor, I. E. (2024). Cyberstalking in Nigeria: An exploratory study of section 24 of the Nigerian cybercrimes (prohibition, prevention, etc.)(amendment) act, 2024. *International Cybersecurity Law Review*, *5*(3), 443-458.
24. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN computer science*, *3*(2), 127.
25. Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT express*, *8*(3), 313-321.
26. Chougule, H., Dhadiwal, S., Lokhande, M., Naikade, R., & Patil, R. (2022). Digital evidence management system for cybercrime investigation using proxy re-encryption and blockchain. *Procedia Computer Science*, *215*, 71-77.
27. Ratul, M. H. A., Mollajafari, S., & Wynn, M. (2024). Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution. *Sustainability*, *16*(24), 10885.
28. Schardong, F., & Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. *Sensors*, *22*(15), 5641.
29. Nita, S. L., & Mihailescu, M. I. (2024). A novel authentication scheme based on verifiable credentials using digital identity in the context of Web 3.0. *Electronics*, *13*(6), 1137.
30. Dave, G., Choudhary, G., Sihag, V., You, I., & Choo, K. K. R. (2022). Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, *112*, 102516.
31. Sætra, H. S. (2022). The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security. *Technology in Society*, *68*, 101854.
32. Onwuadiamu, G. (2025). Cybercrime in criminology; a systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, 100136.
33. Ranchordás, S. (2024). The invisible citizen in the digital state: administrative law meets digital constitutionalism. In *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era* (pp. 15-40). The Hague: TMC Asser Press
34. Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(03), 1542-1556.

35. Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327-350.
36. Bekkers, L., van't Hoff-De Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, *127*, 103099..
37. Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.
38. Onota, E. O., AC-Ogbonna, C., & Alfred-Igbokwe, N. (2024). Cross-border migration, banditry and the challenges of development in Nigeria. *Discover Global Society*, *2*(1), 80.
39. Kalogiannidis, S., Paschalidou, M., Kalfas, D., & Chatzitheodoridis, F. (2023). Relationship between Cyber Security and Civil Protection in the Greek Reality. *Applied Sciences*, *13*(4), 2607.
40. Rughiniș, R., Bran, E., Stăiculescu, A. R., & Radovici, A. (2024). From cybercrime to digital balance: How human development shapes digital risk cultures. *Information*, *15*(1), 50.
41. Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. *Information*, *16*(5), 336.
42. Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization*, *12*, 100268.
43. Baho, S. A., & Abawajy, J. (2023). Analysis of consumer IoT device vulnerability quantification frameworks. *Electronics*, *12*(5), 1176.
44. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273.
45. Woods, D. W., & Walter, L. (2022, June). Reviewing estimates of cybercrime victimisation and cyber risk likelihood. In 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 150-162). IEEE.
46. Ige, O. (2023). Trends of cybercrime from 2001 to 2021: cybersecurity action plan for Papua New Guinea. Discover Global Society, 1(1), 9.

47. Bernik, I., Prislan, K., & Mihelič, A. (2022). Country life in the digital era: Comparison of technology use and cybercrime victimization between residents of rural and urban environments in Slovenia. Sustainability, 14(21), 14487.

48. Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. Societal Impacts, 1(1-2), 100013.

49. Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. Computers & security, 141, 103826.

50. Ali, A., Shah, M., Foster, M., & Alraja, M. N. (2025). Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country. Computers, 14(2), 38.

51. Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. Asian Journal of Criminology, 19(3), 419-439.

52. Mushtaq, S., & Shah, M. (2024). Critical factors and practices in mitigating cybercrimes within e-government services: A rapid review on optimising public service management. Information, 15(10), 619.

53. Minhat, M., Abdullah, M., Dzolkarnaini, N., & Sapiei, N. S. (2023). *Cryptocurrency risk and governance challenges*. Routledge.

54. Strang, K. D. (2024). Cybercrime risk found in employee behavior big data using semi-supervised machine learning with personality theories. Big Data and Cognitive Computing, 8(4), 37.

55. Van Nguyen, T., Truong, T. V., & Lai, C. K. (2022). Legal challenges to combating cybercrime: An approach from Vietnam. Crime, Law and Social Change, 77(3), 231-252.

56. Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: an analysis of the cyber threat landscape and readiness. IEEE Access, 11, 40049-40063.

57. Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. Computer Law & Security Review, 53, 105961.

58. Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. Government Information Quarterly, 39(4), 101679.

59. Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alshehri, A., & Lin, J. C. W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing, 12(1), 38.

60. Hoenig, A., Roy, K., Acquaah, Y. T., Yi, S., & Desai, S. S. (2024). Explainable AI for cyber-physical systems: Issues and challenges. IEEE access, 12, 73113-73140.

61. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7-34.

62. Bentotahewa, V., Hewage, C., & Williams, J. (2022). The normative power of the GDPR: A case study of data protection laws of South Asian countries. SN Computer Science, 3(3), 183.

63. Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2022). A review on cyber crimes on the internet of things. Deep learning for security and privacy preservation in IoT, 83-98.

64. Zhang, Y., & Dong, H. (2023). Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. Journal of Cloud Computing, 12(1), 64.

65. Tok, Y. C., & Chattopadhyay, S. (2023). Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling. Forensic Science International: Digital Investigation, 45, 301540.

66. Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. International Cybersecurity Law Review, 3(2), 255-272.

67. Ahmad, R., & Thurasamy, R. (2022). A Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes. Journal of Cyber Security and Mobility, 11(3), 405-432.

68. Al-Suqri, M. N., & Gillani, M. (2022). A comparative analysis of information and artificial intelligence toward national security. IEEE Access, 10, 64420-64434.

69. Kassa, Y. W., James, J. I., & Belay, E. G. (2024). Cybercrime intention recognition: A systematic literature review. Information, 15(5), 263.

70. Martineau, M., Spiridon, E., & Aiken, M. (2023). A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature. Forensic Sciences, 3(3), 452-477.

71. Tubaishat, A., & AlAleeli, H. (2024). A Framework to Prevent Cybercrime in the UAE. Procedia Computer Science, 238, 558-565.

72. Mara, D., Nate, S., Stavytskyy, A., & Kharlamova, G. (2022). The place of energy security in the national security framework: an assessment approach. Energies, 15(2), 658.

73. Godsell, D., Lel, U., & Miller, D. (2023). US national security and de-globalization. Journal of International Business Studies, 54(8), 1471-1494.

74. Cevik, S. (2025). Navigating minefields and headwinds: National security, demographic shifts, climate change and fiscal policy in Lithuania. Asia Europe Journal, 1-22.

75. Singh, P. P., & Philip, D. (2023). Modelling & analysis of high impact terrorist attacks in India & its neighbors. ISPRS International Journal of Geo-Information, 12(4), 162.

76. Samusevych, Y., Lyeonov, S., Artyukhov, A., Martyniuk, V., Tenytska, I., Wyrwisz, J., & Wojciechowska, K. (2023). Optimal design of transport tax on the way to national security:

Balancing environmental footprint, energy efficiency and economic growth. Sustainability, 15(1), 831.

77. Villegas-Ch, W., & García-Ortiz, J. (2023). Toward a comprehensive framework for ensuring security and privacy in artificial intelligence. Electronics, 12(18), 3786.

78. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN computer science, 3(2), 127.

79. Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors, 22(3), 1109.

80. Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. IEEE communications surveys & tutorials, 25(1), 319-352.

81. Gosselin, R., Vieu, L., Loukil, F., & Benoit, A. (2022). Privacy and security in federated learning: A survey. Applied Sciences, 12(19), 9901.

82. Wang, Y., Su, Z., Guo, S., Dai, M., Luan, T. H., & Liu, Y. (2023). A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. IEEE Internet of Things Journal, 10(17), 14965-14987.

83. Ramachandra, M. N., Srinivasa Rao, M., Lai, W. C., Parameshachari, B. D., Ananda Babu, J., & Hemalatha, K. L. (2022). An efficient and secure big data storage in cloud environment by using triple data encryption standard. Big Data and Cognitive Computing, 6(4), 101.

84. Liu, Z., Guo, J., Yang, W., Fan, J., Lam, K. Y., & Zhao, J. (2022). Privacy-preserving aggregation in federated learning: A survey. IEEE Transactions on Big Data.

85. Padyab, M., Padyab, A., Rostami, A., & Ghazinour, M. (2024). Cybercrime in Nordic countries: a scoping review on demographic, socioeconomic, and technological determinants. *SN Social Sciences*, *4*(11), 205.

86. Bharti, Alka (2023) Copyright Infringement in Cyber Space With Reference To Information Technology Act 2000 A Critical Study. http://hdl.handle.net/10603/567518

87. Dilip Kumar (2022) Inchoate crimes under Indian penal code with special reference to UK and India a study. http://hdl.handle.net/10603/471215.

88. Dimpal Goyal (2025) the tampering of evidence in trial of cases under indian evidence act 1872 a study of emerging problems and solutions. http://hdl.handle.net/10603/667130.

89. Dwivedi, Divya (2024), Data Privacy and Public Service Delivery in India a Critical Legal Study. http://hdl.handle.net/10603/664722.

90. Pech, L. (2022). The rule of law as a well-established and well-defined principle of EU law. *Hague Journal on the Rule of Law*, *14*(2), 107-138.

91. Graves, J. T., & Acquisti, A. (2023). An empirical analysis of sentencing of "Access to Information" computer crimes. *Journal of Empirical Legal Studies*, *20*(2), 434-471.

92. Haughton, S. A., & Romaniuk, S. N. (2023). Civil Liberties and Homeland Security. In *The Handbook of Homeland Security* (pp. 525-531). CRC Press.

93. Maras, K., Sweiry, A., Villadsen, A., & Fitzsimons, E. (2024). Cyber offending predictors and pathways in middle adolescence: Evidence from the UK Millennium Cohort Study. *Computers in Human Behavior*, *151*, 108011.

94. Smt. Shwetha P (2022) A Comparative Study of Right To Privacy In UK USA and India With A Special Reference To Data Protection. http://hdl.handle.net/10603/556930

95. Krishnamoorthy,R (2025) A Novel Technique in Enhancing Security of Electronic Medical Record Cloud Storage System Based on GDPR with Blockchain Techniques. http://hdl.handle.net/10603/636564.

96. Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105336.

97. Mamta Soni (2033) National Security Preventive Detention and Fundamental Rights A Complex Trilogy An Analytical Study in Human Rights Perspective. http://hdl.handle.net/10603/622469

98. Rawal, Sonal (2024), A Comparative Study Of Cyber Laws With Reference To India And The USA . http://hdl.handle.net/10603/572167.