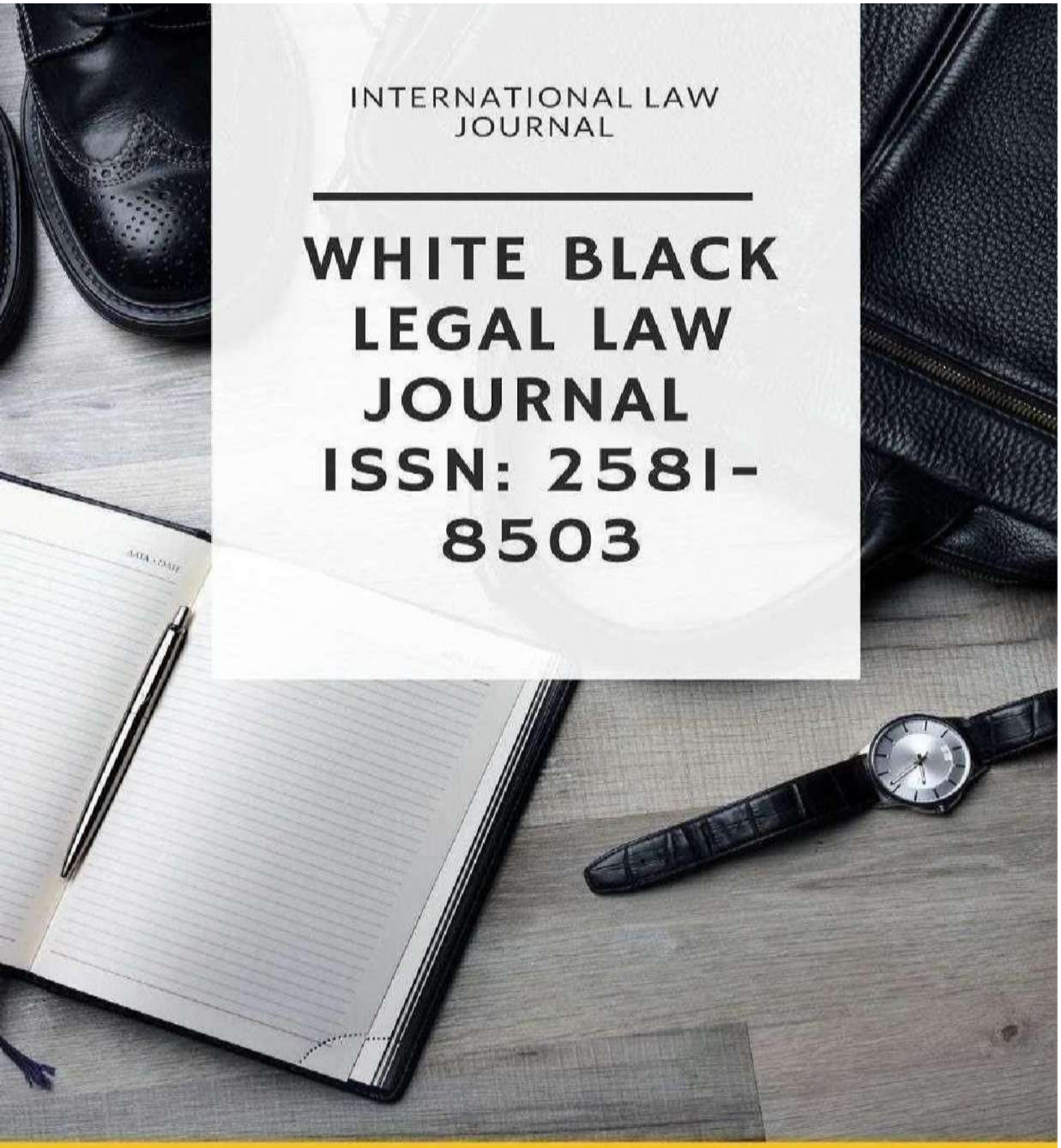

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

THE LAWS REGULATING CYBER CRIMES IN INDIA, THE USA AND THE EU: AN ANALYSIS

AUTHORED BY - POOJA KASHYAP

LLM (BUSINESS LAW)

Enrolment No.: A0319324035 Batch: 2024-25

Research Dissertation submitted to Amity Institute of Advanced Legal Studies
Amity University Uttar Pradesh

In Part Fulfilment of Requirement for the Degree of Master of Laws (LLM)

Under the Supervision of Dr. Mishal Qayoom Naqshbandi
(Assistant Professor)

DECLARATION

I, **Pooja Kashyap**, hereby declare that the dissertation titled **"The laws regulating Cyber Crimes in India, The USA and The EU: An Analysis"** submitted to the **Amity Institute of Advanced Legal Studies**, **Amity University Uttar Pradesh**, is a result of my original work and has been completed in partial fulfilment of the requirements for the degree of **Master of Laws (LLM)**. The work presented in this dissertation is entirely my own, and no part of it has been copied from any other source, except for references duly acknowledged.

I also declare that the work is based on the study, analysis, and research carried out by me, under the supervision of **Dr. Mishal Qayoom Naqshbandi** (Assistant Professor), and has not been submitted for any other degree or award at any other institution.

I hereby declare that the dissertation is my original work and has been carried out independently.

Signature:

Pooja Kashyap Enrolment No.: A0319324035

Batch: 2024-25

CERTIFICATE

This is to certify that this dissertation entitled " The laws regulating Cyber Crimes in India, The USA and The EU: An Analysis " which is being submitted by Pooja Kashyap Enrolment No: A0319324035, LLM (Business Law) for the award of degree of Masters in Law is Bonafide research. She has worked on the above topic under my constant supervision and guidance to my entire satisfaction and her dissertation is complete and ready for submission. I am satisfied that this dissertation is worthy of consideration for the award of Degree of Masters in Law. As this dissertation meets the requirements laid down by Amity University, Noida for awarding the Degree of Masters in Law, I recommend that this dissertation may be accepted for the evaluation by the University.

Date:
Place: Noida

Dr. Mishal Qayoom Naqshbandi
(Assistant Professor)

(AIALS)

Amity University, Noida, Uttar Pradesh

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to **Dr. Mishal Qayoom Naqshbandi**, Assistant Professor at the **Amity Institute of Advanced Legal Studies**, for her continuous guidance, valuable support, and encouragement throughout the process of researching and writing this dissertation. Her expertise, suggestions, and unwavering support have been invaluable in the completion of this work.

I would also like to extend my heartfelt thanks to the faculty members and administrative staff at the **Amity Institute of Advanced Legal Studies**, Amity University Uttar Pradesh, for their support and resources that helped me in the successful completion of my research.

I express my deep gratitude to my family and friends for their constant encouragement and support during my academic journey. Their patience, understanding, and love have been a source of great strength.

Lastly, I would like to acknowledge all those whose work has been referred to in this dissertation, as well as those who have contributed directly or indirectly to this research. Their contributions have been a great help in shaping my understanding of the subject.

Thank you all for your contributions and support.

DATE: **Signature**

PLACE: NOIDA Pooja Kashyap

Enrolment No.: A0319324035

Batch: 2024-25

LIST OF ABBREVIATION

AIR	All India Reporter
Art.	Article
CERT-In	Indian Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act
DOS	Denial of Service
ECPA	Electronic Communications Privacy Act
EU	European Union
GDPR	General Data Protection Regulation
IPC	Indian Penal Code
IT	Information Technology Act
SC	Supreme Court
SCC	Supreme Court Cases
SCJ	Supreme Court Journals
Sec.	Section
Supra	Above
UOI	Union of India
Vol.	Volume
Vs.	Versus

LIST OF CASES

TABLE OF CONTENT

ABSTRACT

Cybercrimes denote a category of illegal activities done in the digital space, which encompasses a diverse range of illegal activities committed using computers, network and the internet. These offences use technological vulnerabilities to breach data, privacy, or disrupt digital systems. Some of the examples including hacking, identity theft, phishing etc. As we become more reliant on technologies so does the cybercrimes, which makes it necessary to have cyber security measures and legal framework with respect to that. With the transition to electronic mode, technology has dominated the world. As information spreads freely in cyberspace, countries prioritize data protection for national benefit and public interest. Each country has its own style and legal framework in regulating and controlling cybercrime. Thus, this paper is an attempt to understand and analyses the cyber laws of India and to compare with the laws of USA and EU. This comparative analysis focuses on the unique socio-economic and legal contexts of each region and highlight the similarities and disparities in regulating cybercrime. The exponential growth of the internet has given rise to an increase in cybercrime, necessitating robust legal frameworks across jurisdictions. This paper provides a comparative analysis of the laws regulating cybercrime in India, the USA, and the European Union (EU). India's Information Technology Act, 2000, serves as the cornerstone for addressing cybercrime, focusing on data protection, hacking, and identity theft. In contrast, the USA employs a multifaceted approach, with federal laws such as the Computer Fraud and Abuse Act (CFAA) and state-level regulations, offering comprehensive coverage against diverse cyber threats. The EU, under the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) Directive, emphasizes data privacy and cross-border cooperation for combating cybercrime. This study examines the scope, enforcement mechanisms, and international cooperation facilitated by these legal frameworks, highlighting their effectiveness and challenges. The analysis reveals disparities in enforcement strategies and cross-jurisdictional coordination, emphasizing the need for global harmonization. Recommendations include enhancing collaborative frameworks, adopting uniform definitions of cybercrimes, and fostering international treaties to counter emerging threats.

Keywords*:* *Cybercrime, India, USA, European Union, IT Act, CFAA, GDPR, legal frameworks, data protection, international cooperation, cybersecurity.*

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

In the digital age, cybercrimes have become one of the most significant threats to global security, economy, and privacy. The rapid development of technology and the expansion of the internet have led to an increase in cybercrimes such as hacking, identity theft, cyber terrorism, and online fraud. Governments worldwide are tasked with creating effective laws to combat these crimes, but due to the transnational nature of cyber offenses, legislation often lags behind technological advancements. This chapter introduces the legal frameworks regulating cybercrime in three significant jurisdictions: India, the USA, and the European Union (EU), exploring the evolution of cybercrime laws in these regions and their efforts to address new challenges in cyberspace. The comparative analysis of these regions will offer valuable insights into the strengths, weaknesses, and areas of improvement in the global fight against cybercrime.[1]

Cybersecurity is a continually evolving field, driven by the constant emergence of new threats and technological advancements. The imperative is to stay ahead of cyber adversaries through heightened vigilance. In the era of digital transformation, cybersecurity has become an increasingly vital technology for safeguarding both individual and business interests. It involves protecting computer system networks and online data from illicit activities such as theft, phishing, Trojans, malware attacks, unauthorized data access, and damage.

The major difference in cybercrime is that the it is difficult to locate the criminals as the cybercrimes don't have proper jurisdiction. The general conception of the people that cybercrimes can be conducted only in online platforms. It has always been a myth. But the reality is that it can be conducted without the involvement in the cyberspace. Software Privacy can also be taken as an example.[2]

The Cybersecurity is a continually evolving field, driven by the constant emergence of new threats and technological advancements. The imperative is to stay ahead of cyber adversaries through heightened vigilance. In the era of digital transformation, cybersecurity has become an increasingly vital technology for safeguarding both individual and business interests. It involves protecting computer system networks and

[1] Prabhash Dalei and Tannya Brahme, Cyber Crime and Cyber Law in India: An Analysis, IJHAS Vol.2 No.4, 106 (2013)
[2] Yoshita Gandhi, "Cyber laws: Comparative study of Indian law & Foreign laws," Vol 1 JAL&J (2020)

online data from illicit activities such as theft, phishing, Trojans, malware attacks, unauthorized data access, and damage. The primary goal of cybersecurity is to preserve the confidentiality of digital assets, as individuals, businesses, and governments face growing susceptibility to cyberattacks due to their escalating reliance on the internet. Any crime which are committed in digital space is cybercrime.

The term cybercrime has no specific explanation given in any resolution or legislation in India. The general understanding is that the crime is conducted in the digital space is coined as a cybercrime. Cybercrime is easy to commit (if one has the know how to do it), hard to locate in jurisdictional terms, given the geographical indeterminacy of the net1. Therefore, it stands to reason that "cyber-crimes" are offenses relating to computers, information technology, the internet, and virtual reality. The assaults focus on the corporate or individual virtual body, which is the assortment of instructive qualities that portray people and associations on the Web, instead of an actual body. Cybercrime affects multiple individuals. Cybercrimes, such as financial theft, espionage, and other cross-border crimes, are committed globally by both state and non-state actors. Cyber warfare is basically a cybercrime that between one nation state and international cross borders. [3]John Odumesi (2014) characterize Cybercrime as "a crime that has to do with the abuse of digital resources in a cyberspace or via the internet or network networks, wither through wired or wireless communication."

The major difference in cybercrime is that the it is difficult to locate the criminals as the cybercrimes don't have proper jurisdiction. The general conception of the people that cybercrimes can be conducted only in online platforms. It has always been a myth. But the reality is that it can be conducted without the involvement in the cyberspace. Software Privacy can also be taken as an example. Cybercrimes can be classified into different categories. It includes cybercrime against individuals, cybercrime against organization, cybercrime against society. Cybercrime against individuals are the types of crimes which are basically targeting persons or individuals. Some of the examples for these types of cybercrimes are cyber defamation, phishing, email spoofing, spyware etc.
[4]

[3] John Odumesi – Information Technology Analyst
[4] Animesh Sarmah, Roshmi Sarmah, Amlan Jyothi Baruah, A Brief Study of Cyber Crime and Cyber Laws in India, IRJET 1633 (2017)

Cyber defamation is basically means, any activities conducted by a person to damage the reputation of an individual or group of persons. Cyber Defamation is defaming someone in cyberspace. Posting defaming comments on social media platform is one of the best examples for cyber defamation. Another example, which is Phishing, is when attackers send scam emails (or text messages) that contain links to malicious websites. [5]

The websites may contain malware (such as ransomware) which can sabotage systems and organizations. Or they might be designed to trick users into revealing sensitive information (such as passwords), or transferring money. It is basically a fraudulent practice to gain confidential information pretending to be legitimate source.

Email Spoofing is one of the common forms of cybercrime. [6]Email Spoofing is basically a threat that involves sending email messages with a fake sender address.[7] It is an activity in which sender fake his identity to gain trust of the receiver. Spyware is a software which is having malicious characteristics. Such software collects data without having authority and sent to third party without the consent. Spyware collects personal and sensitive information that it sends to advertisers, data collection firms, or malicious actors for a profit Attackers use it to track, steal, and sell user data, such as internet usage, credit card, and bank account details, or steal user credentials to spoof their identities.[8]When it comes to cybercrime against organization, the main motive of the cyber attackers to target organizations to gain highly confidential information from both private and public organizations.

These types of attacks are majorly carried out in a massive scale in order to obtain lump sum amount. It includes web Jacking, salami attack etc. web jacking means the attacker send a fake link to the receiver and when the receiver opens, it will direct to the fake page. This type of offence helps to get access or control of sites without any authority and Salami Attack is a type of offence also referred as Salami Slicing. In this method, the attacker steals little money amount of money which lead the offence to go unnoticed.

[5] National Cyber Security Centre, https://www.ncsc.gov.uk/guidance/phishing#:~:text=Business%20Guide%20beforehand.-,What%20is%20phishing%3F,can%20sabotage%20systems%20and%20organisations.

[6] Fortinet, https://www.fortinet.com/resources/cyberglossary/email-spoofing

[7]Fortinet,https://www.fortinet.com/resources/cyberglossary/spyware#:~:text=Spyware%20is%20malicious%20software% 20that,device%20without%20the%20user's%20consent.

[8] Id.

Cybercrime against society includes cyber terrorism and cyber espionage.[9] Cyber Terrorism is also known as Digital Terrorism. These attacks are done by recognized terrorist organization against computer system with an intention of generating alarm, panic or the physical disruption of the information system. Some of the examples are targeting and attacking financial institution to Transfer money and cause terror, virus on vulnerable networks, any kind of terror threats using internet. Cyber Espionage are the type of attack which are conducted to gain political or economic gain. Cyber espionage is primarily used as a means to gather sensitive or classified data, trade secrets or other forms of IP that can be used by the aggressor to create a competitive advantage or sold for financial gain.[10]

In the scenario of technological development, around the world, it is rapidly growing in a very positive way. But along with that few anti things also comes to the limelight. One of the aspects is rapid growth of digital and network technology, which helped in developing a virtual world of cyberspace. Cyber space brings great boomin every field of lifestyle and economy but parallel to the same, there is a growth of new crime, which is called cybercrime. The internet was originally designed as a medium for science and knowledge exchange, but it is now used by both the victim and the perpetrator to conduct cybercrime. Communication, ecommerce, and e-governance became more transactional as time went by.[11] Cyber rules cover all compliance questions pertaining to internet violence. As the number of Cybercrime such as unauthorized access and hacking, Trojan attack, virus and worm attack, denial of service attacks etc. are increasing; the need for related laws and their application has also gathered great force. Cybercrime has neither the origin, nor the reference in the law.

(a) Cybercrime in a broader sense which is computer related crime any illegal behaviour committed by means of an operating system or network, including such On the tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to cyber space, cybercrime was divided into two categories and defined thus:

[9]Wigan Council, https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyberterrorism.aspx#:~:text=What%20is%20cyber%20terrorism%3F,disruption%20of%20the%20information%20sy stem.
[10] CrowdStrike, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/
[11] Yougal Joshi and Ananda Singh, "A Study of Cyber Crime and Security Scenario",International Journal of Engineering and Management Research, vol.3 (3) June, 2013, pp.13-18

(b) Cybercrime in a narrow sense that is computer crime in which any illegal behaviour done by the means of electronic operations that targets the security of computer systems and the data processed.

Crimes as illegal possession or distributing information by means of a computer system or network.

According to the tactical aspect attacks to digital networks for the purpose of seizing control or even destroying infrastructures that are vital to governments and sectors are of the crucial importance. According to the Norton report frequency of cyber attacks on Indian assets, with the government and private infrastructure equally exaggerated. In July 2013 government published national cyber security policy and just after that it was reported that government official's emails had been hacked. The NCSP is far from answering all nuances of the cyber threat. It doesn't maximize its potential for optimum benefit it just only provides guidelines for the standard operating procedure. The crucial point of security concern related to telecom industry which is fully integrated into cyberspace is missing.[12]

The advancement in technology has resulted in an increase in illegal activity, and the IT Act of 2000 establishes procedures for dealing with cybercrime. This model has some advantages in terms of e-commerce, but it does not fix any of the challenges and issues immediately.

In this a steady increase in number of such crimes in this area is expected which demands for greater attention of lawmakers.

- **Combating cybercrime**

The application of technical solutions to combat cybercrime has always been the preferred option for most cybersecurity experts. However, most law enforcement personnel are not equipped with the requisite technological knowledge while most cybercriminals are experts in computer technology.

Various organisations, such as the United States Department of Justice (DOJ) and the International Telecommunication Union (ITU), have initiated capacity building programmes for developing countries in Africa, the Caribbean, and Pacific as well as

[12] Ravikumar S. Patel and Dr.DhavalKathiriya, "Evolution of Cybercrimes in India" International Journal of Emerging Trends & Technology in Computer Science, vol.2 (4) July – August 2013.

other countries in legislative drafting and prosecution of cybercrime. As measures to combat cybercrime continue to multiply, various organisations have established their individual structures for cybersecurity.

It is not uncommon for private organisations to have their own in-house rules on the acceptable use of their networks and also to educate their clients or staff on the issues of cybercrime. Some groups of organisations have also set up Computer Emergency Response Teams (CERTs) to assist in the technical handling of cybercrime, especially those targeted at computer networks. Several multinational organisations have also contributed to the fight against cybercrime.

These organisations have a unique role as some of them control the infrastructure on which the Internet runs, and include the US National Cyber Security Alliance and INTERPOL. Other regional legal instruments include: the League of Arab States Convention on Combating IT Offences (2010), the Shanghai Cooperation Organisation Agreement on Cooperation in the Field of International Information Security, and the African Union Convention on the Confidence and Security in Cyberspace (2014).

On the global level, the United Nations Office on Drugs and Crime (UNODC) is the leading organisation, with a set of international instruments to fight cybercrime. Since cybercrime often involves an organised approach, the UNODC's Convention against Transnational Organised Crime could be used in the fight against cybercrime. Additionally, Interpol facilitates a global network of 190 national police organisations, which plays a key role in the cross-border investigation of cybercrime. The ITU hosts the World Summit on the Information Society (WSIS) implementation process in cybersecurity, labelled the ITU Global Security Agenda.

- **Prevalence and Impact**

The prevalence of cyber frauds has grown exponentially in recent years, as more individuals and organizations shift towards online platforms for personal and business activities. As of 2023, global reports indicate that cybercrime, including fraud, has become one of the largest threats to economic and social stability, with losses running into billions of dollars annually. The ease of access to digital platforms, combined with the increasing sophistication of cybercriminals, has made it difficult to track and prevent these crimes.

According to the Cybersecurity and Infrastructure Security Agency (CISA), cybercrime is responsible for financial losses of over 10 trillion globally, a number expected to grow substantially in the coming years. The FBI's Internet Crime Complaint Center (IC3) reported over 800,000 complaints related to cyber fraud in the United States alone in 2022, with reported financial losses exceeding 7 billion. In India, the National Crime Records Bureau (NCRB) has documented a steady increase in the number of cybercrimes, with cyber frauds forming a significant portion of these statistics. The rise in online transactions, particularly during and after the COVID-19 pandemic, has further exacerbated the situation.

1.3 STATEMENT OF PROBLEM

Despite the growing prevalence of cybercrime, there is a lack of cohesive global legal standards to regulate it effectively. Each jurisdiction—India, the USA, and the EU—has implemented its own set of laws and regulations to address cybercrime, resulting in varying degrees of legal protection and enforcement mechanisms. The problem lies in understanding how these different legal frameworks intersect, their effectiveness in combatting cybercrime, and the challenges of enforcement across borders.

This study seeks to address these issues by analysing and comparing the legal provisions in each of these jurisdictions and identifying areas where improvements can be made to create a more unified and effective approach to cybercrime regulation

1.4 RESEARCH OBJECTIVES

The main objectives of this dissertation are:

- To analyses the legal frameworks regulating cybercrime in India, the USA, and the EU, focusing on relevant statutes, regulations, and enforcement mechanisms.
- To compare and contrast the approaches taken by these jurisdictions in addressing different types of cybercrime.
- To identify the challenges in enforcing cybercrime laws, including issues of jurisdiction, technological complexity, and international cooperation.
- To examine the role of privacy and data protection laws in regulating cybercrime and their impact on investigations and prosecutions.
- To evaluate the effectiveness of preventive measures, such as cybersecurity frameworks and policies, in preventing and mitigating cybercrime.

- To offer policy recommendations for improving the regulation and enforcement of cybercrime laws globally.

1.5 RESEARCH QUESTIONS:

- What are the key similarities and differences in the legal frameworks governing cybercrime in India, the USA, and the European Union?
- How effective are the enforcement mechanisms in addressing cybercrime within each jurisdiction, and what challenges do they face?
- To what extent do India, the USA, and the European Union promote international cooperation in combating cross-border cybercrime?
- How do specific laws, such as India's IT Act, the USA's CFAA, and the EU's GDPR, address emerging cyber threats like ransomware, phishing, and data breaches?
- What recommendations can be made to harmonize the cybercrime laws of India, the USA, and the EU for improved global cybersecurity governance?

1.6 LITERATURE REVIEW

Books

"Cybercrime and Digital Disputes" by Dr. K. S. P. Raghavan

This book provides a comprehensive analysis of the legal issues related to cybercrime, including the Indian context. It explores the provisions of the Information Technology Act, 2000 and its amendments in India, addressing the various categories of cybercrime. The book will serve as a primary reference for understanding Indian cybercrime laws and the enforcement challenges within the country.

"Cybercrime: Law and Regulation" by S. K. Verma and K. M. Nair

This book delves into the legal, regulatory, and procedural aspects of cybercrime. It offers a detailed discussion on global legal standards, particularly focusing on the legislative measures adopted by the USA, the EU, and India. It is essential for the comparative legal analysis of the cybercrime laws in these regions.

"Computer Crime Law" by Orin S. Kerr

Orin Kerr's book provides a thorough examination of the law governing computer- related crimes in the USA. It covers statutes such as the Computer Fraud and Abuse Act (CFAA), case law, and recent legal developments in the fight against cybercrime. This

book is highly relevant for understanding the legal mechanisms regulating cybercrime in the USA and the challenges of enforcement in the digital age.

"The Law of Cybercrimes and Their Investigation" by S. K. Sharma

This book offers an overview of the law governing cybercrimes in India and the international legal frameworks for combating these crimes. It also discusses the procedural and investigative aspects of cybercrimes. It is particularly useful for understanding the investigative challenges and the legal protections in place in India.

"European Cybercrime Legislation: A Critical Analysis" by José L. Gutiérrez

This book analyzes the European Union's approach to regulating cybercrime, focusing on the Directive on Attacks Against Information Systems and the General Data Protection Regulation (GDPR). It critically assesses the effectiveness of the EU's legal framework in combating digital threats. Essential for understanding the EU's unique approach to cybercrime regulation and privacy concerns.

"Cybercrime and Digital Forensics: An Introduction" by Thomas J. Holt and Adam

M. Bossler

This book provides a foundational introduction to cybercrime, digital forensics, and the legal processes involved in investigating and prosecuting cybercrimes. It includes discussions on international law, enforcement challenges, and the role of digital forensics in cybercrime investigations. Useful for understanding the intersection of cybercrime laws with investigative processes and digital forensics.

CASE LAWS:

Ms. Jyothi Jain & Rashmi Chaudhary, understanding the concept of cybercrimes In India VIS-À-VIS Cyber Laws of USA

This article provides extensive laws about the idea of the IT Act and compares the laws With the USA. The paper is an attempt to compare the Indian present status of cyber Legislation with the legislation of the USA for understanding and exploring the deficiencies and inadequacies of Indian Cyber laws. The article starts with a basic introduction and explains the concept of cybercrime. Then slowly explore the Indian legislation and interpret the concept of USA Cyber Crimes Laws. The author analyses the laws of each country and understands the drawbacks of Indian legislation concerning tackling cybercrimes. The Author finds the Indian law as a gap-filler and many forms of cybercrimes have to be addressed.

Prabhash Dalei and Tannya Brahme, Cyber Crime, and Cyber Law in India: An Analysis Vol 2 IJHAS

The article is an attempt to explain the cyber laws in India by explaining every section Of the relevant IT Act 2000. Along with the primary law, the article explains the concept Of cybercrime and the government initiatives to curb cybercrimes in India. The article Starts with an introduction and briefly explains different forms of cybercrime and the Concept of cybercrime in a very wide manner. The author has attempted to give his Analysis of the cybercrime laws in India. According to the author, Indian laws Concerning cybercrimes are just to fill the gap. There is still room left to improve and Frame laws for the evolving purpose of cybercrime.

Yoshita Galwani, Cyber Laws: Comparative Study of Indian and Foreign Laws JAL&J

The article explores the law of Indian cybercrime and gives an overview of the Important provisions of the IT Act. The overview of the relevant provisions under the IT Act was explained under the subheadings of adjudication, e-commerce, and e- Governance, and digital signature. The paper attempts to explain the Cyber Security Policy 2013 and National Cyber Security Strategy 2020. The author briefly explains the Concept of different types of cybercrimes and cyber-attacks in India. The author has Included the time of Covid 19 as a relevant time in the digital era and that period was India saw a tremendous shift in the use of technology right from online classes to online Shopping. The author explains the laws of the USA, UK, and Australia and compares Them with Indian laws.

Ekadshi & Deepti Monga, Comparative Analysis of Cybersecurity laws of India, the United States and the United Kingdom Vol 9 IJL

This article analyses the cybersecurity laws of India in comparison with the laws of the USA and UK. The objective of this paper is to compare and analyses the current Legislation concerning cybersecurity. The research of this article is conducted based on The secondary data. The author collected information from various journals, articles, Credible links, etc. The author explains different forms of cybercrimes and mentions And explains different policies and strategies that have been formulated by the Indian Government. The result of his research is that Indian laws concerning cybersecurity are Not adequate. The concept of privacy law of an individual is different from nation to Nation but the details of the same are different.

1.7 HYPOTHESIS:

India's IT Act is primarily centred on digital fraud, hacking, and identity theft, reflecting its evolving digital landscape. The USA employs a comprehensive, decentralized approach with federal and state-level laws like the CFAA targeting various cyber threats. The EU emphasizes data protection and privacy through the GDPR and NIS Directive, fostering cross-border collaboration.

These differences result in challenges for addressing cross-border cybercrimes, necessitating global harmonization for effective cybersecurity governance. The legal frameworks regulating cybercrime in India, the USA, and the EU differ significantly in focus, enforcement mechanisms, and priorities.

1.8 RESEARCH METHODOLOGY

In order to analyse the laws regulating cyber-crime in India, the USA, and the EU, a comparative research methodology will be employed. This will involve studying the relevant legislation, case law, and official documents from each jurisdiction to identify and compare the key provisions and enforcement mechanisms in place to combat cyber- crime. Additionally, interviews with legal experts, law enforcement officials, and other stakeholders in each region may be conducted to gain insights into the practical implementation of these laws and the challenges faced in addressing cyber-crime. The research will also consider the impact of international agreements and cooperation on cyber-crime regulation in these jurisdictions. By adopting a comparative approach, this study aims to provide a comprehensive analysis of the legal frameworks governing cyber-crime in India, the USA, and the EU, and to identify areas for potential improvement and harmonization.

The study has been derived from primary sources such as the critical and landmark Judgements, Acts and Reports of various Commissions, and secondary sources such as authoritative books relating to banking law , journals, and articles. The researcher has also taken the help of secondary sources such as the internet for articles, news etc.

1.9 STUDENT LEARNING OUTCOME

Understanding of Cybercrime Laws:

Students will gain a comprehensive understanding of the legal frameworks governing cybercrime in India, the USA, and the European Union, including their objectives, scope, and enforcement mechanisms.

Comparative Analysis Skills:

Students will develop the ability to critically compare and contrast the similarities and differences in cybercrime laws across these jurisdictions, identifying strengths and weaknesses.

Legal Interpretation:

Students will enhance their skills in interpreting and analysing primary legal documents such as statutes, regulations, and case law related to cybercrime.

Awareness of Global Challenges:

Students will understand the challenges of addressing cross-border cyber threats and the role of international cooperation in combating cybercrime.

Practical Application:

Students will be able to apply theoretical knowledge to assess the effectiveness of existing laws and propose innovative legal solutions to emerging cyber threats.

Ethical and Socio-Legal Awareness:

Students will cultivate an awareness of the ethical, social, and legal implications of cybercrime and the importance of privacy and data protection in the digital age.

1.10 SCHEME OF THE STUDY:

The research study consists of 8 chapters: Chapter 1: Introduction

Chapter 2: Cybercrime Laws in India

A Subject matter expert delivers a lecture on cyber crime and law in India in a detailed but simple and easy-to-understand manner.

Chapter 3: Cybercrime Laws in the USA

Cybercrime laws in the United States include the computer Fraud and Abuse Act (CFAA) and other laws that address specific types of cybercrime.

Chapter 4: Cybercrime Laws in the European Union (EU)

Aims to tackle large scale cyber-attacks by requiring EU countries to strengthen national cyber-crime laws and introduce tougher criminal sanctions.

Chapter 5: Comparative Analysis of Cybercrime Laws in India, the USA, and the EU

India: Governed primarily by the Information Technology Act,2000.

USA: Computer Fraud and Abuse Act (CFAA) and Electronic Communications Privacy Act (ECPA)

EU: The EU prioritizes data protection and privacy, evident in the General Data Protection Regulation (GDPR)

Chapter 6: International Cooperation in Cybercrime

A collaboration between countries, law enforcement, and institutions to fight cybercrime.

Chapter 7: Emerging Trends in Cybercrime

It includes Data Privacy and Protection, Artificial Intelligence and Machine Learning, Crypto currency etc.

Chapter 8: Conclusion & suggestion

CHAPTER 2 CYBERCRIME LAWS IN INDIA

2.1 Introduction

Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber crime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber crime'. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber crime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber crime, about which we will now be discussing in detail. In a cyber crime, computer or the data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber crime.

2.2 Legislation to Tackle Cybercrime in India

There are no specific laws to deal with cybercrime. However, some sections of the IT Act 2000 and judicial interpretations are acknowledged in India. Yahoo! Inc. v. Akash Arora & Anr.[13] was the first case in India related to cybercrime. The Court, in this case on the plea filed by Yahoo, granted the permanent injunction which refrained the defendant Akash Arora from using the trademark of Yahoo.

In Vinod Kaushik & Anr. v. Madhvika Joshi & Ors.,[14] the defendant was accused of accessing the e-mail of her father and father-in-law. The Court held the action unauthorized under Section 43 of the IT Act, 2000 and the defendant was made liable. Information Technology Act, 2000 (ITA- 2000) is India's primary law dealing with cybercrime. It was amended in 2008 as the previous act lacked the provisions required to protect one's sensitive personal information provided electronically. Section 43A [15]was taught in the front, which mandates the corporate body to protect sensitive protection data or information. Without such protection, the body would be liable to compensate

[13] Yahoo! Inc. Vs. Akash Arora & Anr., (1999) 19 PTC 201, Delhi High Court.
[14] Vinod Kaushik & Anr. v. Ms. Madhvika Joshi & Others · 2009 (4) R.C.R · 1992 AIR SCW 846 · 1959 SCR 1111
[15] The Information Technology (Amendment) Act, 2008, § 43A, The Gazette of India, pt. II sec. 1

the aggrieved party. Furthermore, section 72A[16] of the act prescribes the penalty for disclosing the personal data of a party by breaching a lawful contract; it says that "the person may be punished with imprisonment for a term not exceeding three years, or with a fine not exceeding up to five lakh rupees, or with both".

Cybercrime is a real threat to an individual's data privacy, including any kind of data stored virtually, whether sensitive or insensitive. The only law to tackle this issue in India is the already discussed Information Technology Act 2000, as amended by the Information Technology (Amendment) Act 2008, by which the judiciary had also given several landmark judgments. Cyberspace lacks any sense of privacy.

The numerous websites that provide a range of services to their users repeatedly fall short in protecting their personal information. At least three times this year, hackers gained access to the Sony website, which includes the play station and music websites. Numerous pieces of personal information were stolen, and for over a week, consumers were kept in the dark about the breach.

As a consumer, I find it difficult to picture other websites being able to defend themselves from assaults if a major corporation like Sony can't keep its website safe from hackers. A new facet of crime has emerged with the growth of the Internet. The NCRB claims that the IT Act 2000 has given the harmed some relief. Despite this, as the NCRB investigation plainly showed, the IT Act will not totally stop criminals from hacking into websites. The perpetrators of the February 2000 cyberattacks are still at large, and each year there are further attacks on different websites.

Despite advances in passing and putting into practise cyber legislation, cybercrime has not yet been completely eradicated. Governments can only hope that a cybercriminal can be found and punished as there isn't much they can do to stop it. In order to secure their personal information as much as possible, Internet users should be more cautious about the websites they visit and familiarise themselves with their privacy policies.

2.3 Digital Personal Data Protection Act, 2023 (DPDPA)

the Digital Personal Data Protection Act, 2023 (DPDPA) is India’s most recent and comprehensive legislation aimed at regulating the processing of personal data, addressing privacy concerns, and protecting individuals from the misuse of their data. The DPDPA

[16] The Information Technology (Amendment) Act, 2008, § 72A, The Gazette of India, pt. II sec. 1

replaces the Personal Data Protection Bill, 2019, which had been stalled in Parliament. The passage of the DPDPA signifies a major shift in India's approach to data privacy and security, responding to growing concerns about data breaches and cyber fraud.

Key provisions of the DPDPA related to cyber frauds include:

Data Protection and Fraud Prevention:

The DPDPA establishes a robust framework for data protection, requiring organizations to obtain explicit consent from individuals before processing their personal data. This provision directly impacts cyber fraud, as it strengthens controls over the collection and storage of sensitive personal information. By restricting unauthorized access and use of personal data, the law aims to mitigate identity theft, phishing attacks, and other forms of cyber fraud involving data misuse.

Breach Notification:

One of the central features of the DPDPA is the requirement for data fiduciaries (those who control or process personal data) to notify both the Data Protection Board of India (DPBI) and affected individuals in the event of a data breach. Prompt notification allows individuals to take action to safeguard their financial and personal data, reducing the impact of potential fraud.

Rights of Individuals:

The DPDPA grants individuals specific rights, such as the right to access, right to correction, right to erasure, and right to data portability. These rights empower individuals to control their personal data, which is crucial in preventing fraud. For instance, if a person's data is compromised or misused, they have the right to request the deletion or rectification of that data, thereby minimizing the chances of further fraudulent activity.

Accountability and Penalties:

The DPDPA imposes stringent penalties on organizations that fail to comply with its provisions, including hefty fines for non-compliance with data protection requirements. These provisions incentivize companies to invest in stronger cybersecurity measures, reducing vulnerabilities that could lead to fraud.

Although theDPA is a significant step forward in addressing data protection, its effectiveness will depend on the speed of enforcement, awareness campaigns, and inter- agency coordination to deal with emerging fraud techniques.

2.4 The Genesis of IT legislation in India

Mid 90's saw an impetus in globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records ie the data what is stored in a computer or an external storage attached thereto. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record

2.5 IT ACT, 2000 Provisions concerning cyber crime

- **Hacking and Data Theft:**

Sections 40 3 and 66 of the IT Act penalize a number of sports activities beginning from hacking proper right into a computer network, records theft, introducing and spreading viruses thru computer networks, bad laptop structures or computer networks or computer programmers, disrupting any computer or computer device or computer network, denying an accredited person get proper of access to a computer or computer network, bad or destroying statistics living in a computer etc. The maximum punishment for the above offences is imprisonment of as a whole lot as three (3) years or a awesome or Rs. five,00,000 (Rupees five lac) or both.

- **Receipt of stolen property:**

Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen laptop beneficial useful resource or verbal exchange device. This segment requires that the character receiving the stolen property want to have performed so dishonestly or

need to have motive to trust that it have become stolen property. The punishment for this offence underneath Section 66B of the IT Act is imprisonment of as a whole lot as three (3) years or a terrific of as a whole lot as Rs. 1,00,000 (Rupees one lac) or both.

- **Identity theft and cheating by way of personation:**

Section 66C of the IT Act prescribes punishment for identity theft and provides that absolutely everyone who fraudulently or dishonestly makes use of the virtual signature, password or some other unique identification function of some other man or woman might be punished with imprisonment of each description for a term which also can moreover boom to three (three) years and shall moreover be vulnerable to super which also can moreover boom to Rs. 1,00,000 (Rupees one lac).

Section 66D of the IT Act prescribes punishment for `cheating by way of personation by way of using pc useful resource' and provides that any man or woman who via way of manner of any communication device or pc useful resource cheats by way of personation, might be punished with imprisonment of each description for a term which also can moreover boom to three (three) years and shall moreover be vulnerable to super which also can moreover

2.6 IPC Provisions concerning cyber crime

The Indian Penal code 1860 (hereinafter referred to as IPC) is a penalizing legislation in India. After the introduction of IT Act 2000, there were several alterations and amendments were made in IPC. The sections in IPC which are dealing with record and document has been amended by adding the ambit of the term "electronic" thereby treating the electronic records and documents on a par with physical records and documents . The sections in IPC which are dealing with false entry and false document like Sec 192, 204, 463, 468, 474 etc. have been amended since the introduction of IT Act 2000 thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic document just like physical acts of forgery or falsification of physical records. Before the enactment of IT, Act 2000 all the evidence submitted before the court were in the form of physical nature. After the amendment of IEA, 1872, all the physical form of documents included the ambit of electronic document. Thus, the activities which are done in the electronic form is admissible before the court. Sec 65B of the Act provides for the admissibility of electronic records as evidence.

Non coverage of many crimes

2.7 Case studies

Shreya Singhal v. Union of India (2015)[17]

This landmark judgment dealt with the constitutionality of Section 66A of the Information Technology Act, 2000 (IT Act). The provision criminalized the sending of offensive messages through communication services, social media platforms, etc. Shreya Singhal, a student, challenged the law after two women were arrested for making comments on Facebook about a shutdown in Mumbai. The Supreme Court held that Section 66A was unconstitutional as it was vague and overly broad, leading to arbitrary arrests and misuse. The Court emphasized that it violated the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Indian Constitution. This judgment led to the striking down of Section 66A, highlighting the need for laws to be precise and balanced in safeguarding free speech while tackling cybercrimes.

State of Tamil Nadu v. Suhas Katti (2004)[18]

In one of the first cybercrime cases in India, Suhas Katti was convicted for sending obscene and defamatory messages via email and SMS. The case revolved around Section 66A of the IT Act, which deals with the punishment for sending offensive messages. Katti was accused of sending sexually explicit messages to a woman, leading to mental harassment. The court found him guilty and convicted him for sending obscene content under the IT Act. This case set an early precedent for cybercrimes involving harassment and inappropriate content online and marked the beginning of legal actions against cyberbullying and online harassment in India.

People's Union for Civil Liberties (PUCL) v. Union of India (1997)[19]

The case centered on Section 69 of the IT Act, which allowed the government to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in computer systems. The People's Union for Civil Liberties (PUCL) challenged this

[17] Supreme Court of India, Shreya Singhal v. Union of India, Writ Petition (Criminal) No. 167 of 2012, 2015.
[18] Tamil Nadu District Court, State of Tamil Nadu v. Suhas Katti, 2004.
[19] Supreme Court of India, *People's Union for Civil Liberties (PUCL) v. Union of India*, Writ Petition

(Criminal) Nos. 128-132 of 1996, 1997.

provision, arguing that it violated the right to privacy and lacked safeguards against misuse. The Supreme Court held that while the government had the authority to intercept communications under national security concerns, such powers needed to be exercised with judicial oversight and clear procedural safeguards to protect citizens' fundamental rights. This judgment highlighted the balance between national security concerns and individual privacy rights.

Amazon.com Inc. v. Future Group (2020)[20]

This high-profile corporate dispute between Amazon and Future Group revolved around a breach of an agreement concerning the sale of Future Group's retail assets to Reliance Industries. Amazon had acquired a stake in Future Retail in 2019 and had a right of first refusal for the sale of its retail business. When Future Group announced its deal with Reliance, Amazon filed for arbitration, claiming that the deal violated their agreement. The legal battle involved issues of breach of contract, corporate governance, and foreign investment laws. The case brought attention to the complexities of e-commerce contracts in India, and the Delhi High Court granted an interim order, barring Future Group from proceeding with the sale to Reliance. The case highlighted the evolving legal landscape of corporate law and e-commerce in India, especially concerning foreign investment and competition laws.

United States of America:

United States v. Aaron Swartz (2013)[21]

Aaron Swartz, a gifted programmer and activist, downloaded academic articles from JSTOR using MIT's network, aiming to make them freely available. He was charged under the Computer Fraud and Abuse Act (CFAA) with wire fraud and computer fraud, facing severe penalties. The prosecution argued that his actions constituted unauthorized access and theft, regardless of his intent. Swartz's defense countered that he was exercising his right to access information, highlighting the ethical implications of restricting academic knowledge. The case sparked intense debate about prosecutorial overreach and the need for reforms to the CFAA. Tragically, Swartz committed suicide

[20] Delhi High Court, *Amazon.com Inc. v. Future Group*, 2020.
[21] United States District Court for the District of Massachusetts, *United States v. Aaron Swartz*, 2013.)

during the legal proceedings. The case served as a stark reminder of the tension between intellectual property rights and the open access movement. It raised crucial questions about the scope of computer fraud laws and the ethical responsibilities of those who control access to information.

United States v. Morris (1990)[22]

Robert Morris, a Cornell graduate student, created a self-replicating worm that spread rapidly across the early internet, disrupting thousands of computers. The worm exploited vulnerabilities in Unix systems, causing significant damage and raising alarms about network security. Morris was charged under the CFAA, marking one of the first major prosecutions under this law. The prosecution argued that Morris's actions constituted unauthorized access and disruption, regardless of his intent. The defense argued that Morris had no malicious intent and was merely experimenting. However, the court found him guilty, establishing a precedent for prosecuting computer intrusions even without clear evidence of harmful intent. The case highlighted the vulnerabilities of interconnected systems and the need for stricter cybersecurity measures. It played a crucial role in shaping the legal framework for addressing cybercrime in the U.S.

Microsoft Corp. v. United States (2018)[23]

The U.S. government issued a warrant for emails stored on Microsoft servers in Ireland, seeking data related to a criminal investigation. Microsoft challenged the warrant, arguing that it violated international law and the Stored Communications Act (SCA), which they argued did not apply extraterritorially. The government argued that they had the authority to compel U.S.-based companies to produce data regardless of where it was stored. The Supreme Court ruled in favor of Microsoft, holding that the SCA did not apply extraterritorially. This decision highlighted the conflict between national law enforcement and international data privacy. It also led to the enactment of the CLOUD Act, which allows U.S. authorities to access data stored abroad under specific conditions. The case underscored the complexities of cross-border data access and the need for international cooperation in law enforcement.

[22] United States Court of Appeals for the Second Circuit, United States v. Morris, 1990.

[23] Supreme Court of the United States, Microsoft Corp. v. United States, 2018.

United States v. Mitchell (2019)[24]

Joshua Schulte, a former CIA software engineer, was charged with leaking classified information to WikiLeaks. The leaked data included sensitive hacking tools and techniques used by the CIA. The prosecution argued that Schulte's actions compromised national security and endangered intelligence operations. The defense argued that Schulte was a whistleblower exposing wrongdoing within the CIA. The case involved complex technical evidence and raised questions about insider threats and the protection of classified information. Schulte was ultimately convicted, highlighting the challenges of balancing national security with transparency and accountability. The case serves as a reminder of the risks associated with insider threats and the need for robust security measures in intelligence agencies.

European Union:

Google Spain SL v. Agencia Española de Protección de Datos (2014)[25]

A Spanish citizen sought to have search results linking to an auction notice of his repossessed property removed from Google's search engine. The Court of Justice of the European Union (CJEU) established the "right to be forgotten," allowing individuals to request the removal of personal information from search engine results. This ruling balanced data privacy with freedom of information, requiring search engines to remove information that is inadequate, irrelevant, or no longer relevant. The case had a profound impact on online privacy and data protection in the EU.

Council of Europe v. European Union (2014)[26]

This reflects the ongoing dialogue and legal framework between the Council of Europe and the European Union concerning data protection and human rights. It highlights the importance of international cooperation in addressing digital challenges. The case solidified the importance of data protection as a fundamental right within the EU.

Case C-203/15, Tele2 Sverige AB v. Post-och Telestyrelsen (2016)[27]

[24] United States District Court for the Southern District of New York, *United States v. Mitchell*, 2019.
[25] Court of Justice of the European Union, *Google Spain SL v. Agencia Española de Protección de Datos*, Case C-131/12, 2014.
[26] Council of Europe, 2014.

The CJEU ruled that general data retention obligations imposed on telecommunications providers were incompatible with EU law. This decision emphasized the importance of proportionality and necessity in data retention practices. It protected privacy and data protection rights.

Warren v. Google (2019)[28]

A class action lawsuit alleged that Google unlawfully tracked iPhone users. This case addressed online tracking and data privacy, contributing to the ongoing debate about transparency and control over personal data. The case showed the growing legal challenges faced by companies engaging in extensive online tracking.

International Cases:

R v. Hacking Team (2015):[29] The leak of data from Hacking Team, an Italian company selling surveillance software, exposed the global trade in surveillance technology and raised concerns about human rights and privacy. The case highlighted the risks associated with surveillance technology and its use by governments.

United States v. Ross Ulbricht (2015)[30] Ross Ulbricht, the founder of Silk Road, an online black market, was convicted. The case highlighted the challenges of regulating online criminal activity and the legal implications of digital currencies, showing the difficulties of law enforcement in the dark web.

[27] Court of Justice of the European Union. *Tele2 Sverige AB v. Post-och Telestyrelsen*. Case C-203/15. 21 December 2016.
[28] Warren v. Google (2019). *Case No. 5:12-cv-00630-LHK*, United States District Court for the Northern District of California, 2019.
[29] R v. Hacking Team (2015). *Italian Court*, 2015.

[30] United States v. Ross Ulbricht (2015). *United States Court of Appeals for the Second Circuit*, 2015.

CHAPTER 3 CYBERCRIME LAWS IN THE USA

3.1 Introduction

The United States has a multi-layered legal framework for addressing cyber frauds, drawing from federal laws, regulatory agencies, and state-specific legislation. Key components include the Computer Fraud and Abuse Act (CFAA), the role of the Federal Trade Commission (FTC) in consumer protection, and state-specific laws like the California Consumer Privacy Act (CCPA)

The United States of America has enacted various federal and state laws in order to tackle cybercrime laws in the nation as USA is one of the top 10 nation to face immense number of cyberattack daily. There is no specific or uniform law to deal with cybercrimes in USA as state is having the authority to make better laws as compared to federal laws. In USA, Wire Fraud Statute were considered as the first law to prosecute computer criminals [31]

The Counterfeit Access Device and Computer Fraud and Abuse Act 1984 (hereinafter referred as CFAA) is a federal framework which is introduced to tackle computer abuse. It criminalizes various computer-related activities such as accessing without permission a computer system belonging to a bank or the federal government, or using that access to improperly obtains anything of value.[32] The Act came into force on Oct 12, 1984 and provides federal prosecutors with a specific crime tilted "fraud and related activity in connection with computers" to prosecute computer criminal activity.[33] In addition to that, USA is having the Computer Security Act. In 1987, the US Congress led by Jack Brooks enacted the Act reaffirming NIST (National Institute of Standards and Technology), a division of department of commerce, was responsible for security of unclassified, non-military government computer system.[34] The main motive was to maintain proper security standards.

The Department of Homeland Security protects the nation by identifying key components of homeland security such are Counterterrorism, Immigration, Border Security and

[31] Jyothi Jain & Rashmi Chaudhary, Understanding the concept of Cyber Crimes in India vis-à-vis Cyber laws of USA, 6 IJRAR 427, 429 (2019)
[32] USlegal, https://definitions.uslegal.com/c/counterfeit-access-device-and-computer-fraud-and-abuse-act-of1984/
[33] Id
[34]Epic,https://epic.org/computer-security-actof1987/#:~:text=In%201987%2C%20the%20U.S.%20Congress,non%2Dmilitary%20government%20computer %20systems.

Human Trafficking, Cyber security, Disaster Preparedness, Response and Recovery[35] through the Homeland Security Act. The Cyber Security Research and Development Act helps to authorize funding for computer and network security research and development and research fellowship programs and for other purpose.[36]

The Act was enacted with a main objective to establish an agency to regulate cybercrimes and to provide a safer infrastructure in the states of America. The e- Government Act was enacted on 17th December 2002. The intention behind of this Act is to smoothen and promote the government electronic services and helps the citizens of the America for easy access of electronic services. The statutes include within FISMA [37]and CIPSEA[38] . And lastly, the federal law Cyber Security Information Sharing Act (CISA) was enacted in the America to improve the cyber security by providing platform regarding cyber security threats. Cybersecurity Information Sharing Act is proposed legislation that will allow Unites States government agencies and non-government entities to share information with each other as they investigate cyberattacks[39] .

3.2 The Computer Fraud and Abuse Act (CFAA) (1986)

The CFAA is a foundational federal law addressing computer-related fraud and abuse. Initially enacted to combat hacking, it has evolved to cover a wide range of cybercrimes, including fraud using computer systems. The key provisions are:

1. **Unauthorized Access to Computer Systems:** The CFAA criminalizes unauthorized access to protected computer systems, including using deception or fraud to gain access (e.g., hacking into financial systems).

2. **Fraud and Misuse of Information:** The law specifically targets instances where individuals access computers to commit fraud or steal sensitive information. This includes the use of phishing schemes to obtain login credentials and other financial frauds.

3. **Damaging Systems or Data:** It also criminalizes the intentional damaging of data or systems, which may be linked to fraudulent activities such as deleting financial records or spreading malware.

[35]Onlinewilder, https://onlinewilder.vcu.edu/blog/what-is-homeland-security/
[36] Govinfo, https://www.govinfo.gov/app/details/COMPS-1842
[37] Federal Information Security Management Act 2000
[38] Confidential Information Protection and Statistical Efficiency Act
[39] Techtarget, https://www.techtarget.com/whatis/definition/Cybersecurity-Information-Sharing-Act-CISA

While the CFAA was originally designed to target hacking and unauthorized access, its broad language has also been used to address cyber fraud activities, such as exploiting weaknesses in online banking systems or stealing sensitive financial data.

3.3 Federal Trade Commission (FTC) and Consumer Protection Laws

The FTC plays a crucial role in regulating cyber fraud, particularly in terms of consumer protection. The agency enforces laws and regulations aimed at safeguarding consumers from financial fraud, identity theft, and other online scams.

1. **Role of the FTC in Cyber Fraud**: The FTC investigates and takes action against fraudulent practices that target consumers, including deceptive marketing, identity theft, and phishing scams. It educates consumers about how to avoid cyber fraud and provides resources for reporting fraud, as well as offering tools to assist victims in recovery.

2. **Identity Theft and Assumption Deterrence Act (1998):** This act, enforced by the FTC, specifically targets identity theft, a major form of cyber fraud. It criminalizes the act of knowingly using another person's identity without authorization to commit fraud. It requires federal agencies and businesses to take steps to prevent identity theft, such as the implementation of data security measures, and allows individuals to place fraud alerts on their credit reports to prevent further misuse of their identities.

3.4 State-Specific Laws (e.g., California Consumer Privacy Act – CCPA)

While federal laws set broad standards, states like California have implemented additional measures to protect residents from cyber fraud and ensure privacy in the digital age.

- **California Consumer Privacy Act (CCPA)**

Enacted in 2018, the CCPA provides California residents with enhanced control over their personal data. Although primarily a privacy law, its provisions help address cyber fraud by imposing strict requirements on businesses that collect, use, and share personal information. Key Features of this Act are:

1. Consumers have the right to know what personal information is being collected and to request that their data be deleted.

2. The law mandates businesses to implement reasonable security measures to protect consumer data from unauthorized access and fraud.

3. It also allows consumers to opt-out of the sale of their personal information, reducing the risk of data breaches and subsequent fraud.

- Other states have also enacted similar laws, including the New York SHIELD Act (requiring businesses to protect private information), and Virginia's Consumer Data Protection Act (CDPA), further strengthening protections against cyber fraud at the state level

3.5 Case Laws

Cybercrime cases in the United States are handled by various law enforcement agencies, including the FBI, the U.S. Secret Service, and local police departments. These cases can range from hacking, identity theft, data breaches, to online fraud, cyber terrorism, and child exploitation.

Here are some notable cybercrime cases from the U.S. in recent years:

1. United States v. Aleynikov[40]

- **Brief Fact Summary.**

Defendant was arrested and indicted for violating the National Stolen Property Act when, at the end of his employment at Goldman Sachs, heencrypted and uploaded more than 500,000 lines of source code he had written to a server in Germany. Defendant then downloaded the source code to a home computer and late transferred it to a flash drive and laptop. Defendant moved to dismiss the indictment. The district court denied the motion. The jury convicted Defendant. Defendant appealed.

- **Synopsis of Rule of Law.**

The theft of intangible property does not constitute stolen goods, wares, or merchandise within the meaning of the National Stolen Property Act.

- **Facts.**

[40] United States v. Aleynikov676 F.3d 71 (2012)

Sergey Aleynikov (Defendant) was employed for two years as a computer programmer with Goldman Sachs. Defendant's work focused on developing computer source code for the company's electronic-trading system. Under the company's confidentiality policy, Defendant was required to keep all the firm's proprietary information—including intellectual property created by Defendant—confidential. The policy also prohibited Defendant from taking or using any intellectual property he created while employed by Goldman Sachs when Defendant's employment ended. Defendant accepted a new position, and on his last day at Goldman Sachs, he encrypted and uploaded more than 500,000 lines of source code he had written while at Goldman Sachs to a server in Germany. When he returned home, Defendant downloaded the source code from the server to a home computer. Defendant later transferred the source code to a flash drive and laptop. Defendantwas subsequently arrested for violating the National Stolen Property Act (NSPA). At trial, Defendant moved to dismiss the indictment for failure to state an offense, which the district court denied. The district court held that, for purposes of the NSPA, the source code constituted goods that were stolen by Defendant. The court further denied Defendant's argument that the NSPA did not apply to "intangible intellectual property," such as the computer source code. The jury convicted Defendant, and Defendant appealed, arguing that the trial court erred when it denied his motion to dismiss.

- **Issue.**

- **Whether the theft of intangible property constitutes stolen goods, wares, or merchandise within the meaning of the National Stolen Property Act.**

- **Held.**

No. The trial court's ruling is reversed. The theft of intangible property does not constitute stolen goods, wares, or merchandise within the meaning of the National Stolen Property Act.

Discussion.

Tangible property must be taken for there to be deemed a good that was stolen, for purposes of the NSPA. The value or significance of a tangible good is not relevant to a determination of whether the NSPAhas been violated. At least two other federal circuit

courts have also held that intangible property, such as source code does not constitute goods under the NSPA. If, however, the intangible property is transferred to a tangible form at the time of the theft, such as a photocopy or thumb drive, and the perpetrator completes the theft by taking the photocopy or thumb drive with him or her, the perpetrator may be convicted under the NSPA. In this case, Defendant stole intangible property in an intangible format. There is no evidence that Defendant stole anything tangible from Goldman Sachs. Defendant stole intangible source code by uploading it to an outside server in Germany. Although Defendant later transferred the source code to a thumb drive, the NSPAis not violated unless the intangible property is transferred to a tangible form at the time of the theft. Later storage of intangible property in a tangible form does not make the intangible property a stolen good.

2. Equifax Data Breach (2017)[41]

- **Overview**: One of the largest data breaches in history, affecting 147 million Americans. The breach exposed sensitive data, including Social Security numbers, birth dates, addresses, and driver's license numbers.

- **Attackers**: The breach was reportedly caused by a vulnerability in a web application framework that the attackers exploited to access the company's databases.

- **Outcome**: Equifax faced significant backlash and was fined up to 700 million as part of a settlement with the Federal Trade Commission (FTC).

3. The Colonial Pipeline Ransomware Attack (2021)[42]

- **Overview**: In May 2021, a ransomware attack targeted Colonial Pipeline, the largest fuel pipeline operator in the U.S. This led to widespread fuel shortages across the East Coast of the U.S.

- **Attackers**: The attack was attributed to DarkSide, a Russian cybercriminal group that deployed ransomware to lock Colonial's systems and demand a large ransom in Bitcoin.

[41] In re Equifax, Inc. 362 F. Supp. 3d 1295 (N.D. Ga. 2019)

[42] The Colonial Pipeline Ransomware Attack (2021)

- **Outcome**: Colonial Pipeline paid a ransom of about 4.4 million. However, the FBI later recovered a portion of the ransom paid in cryptocurrency.

4. The Capital One Data Breach (2019)[43]

- **Overview**: This breach exposed the personal data of more than 100 million credit card applicants, including names, addresses, credit scores, and more. The breach was caused by a vulnerability in a cloud computing service that Capital One was using.

- **Attackers**: The hacker was a former Amazon Web Services (AWS) employee, Paige Thompson, who exploited the vulnerability.

- **Outcome**: The hacker was arrested and charged with wire fraud and computer fraud. Capital One faced a 80 million fine from the Office of the Comptroller of the Currency (OCC).

5. The Yahoo Data Breach (2013-2014, disclosed in 2016)

- **Overview**: Yahoo was a victim of multiple breaches, with data from over 3 billion accounts being compromised. This included personal information such as names, email addresses, and security questions.

- **Attackers**: The breach was attributed to Russian hackers associated with the Russian government's intelligence agency, the FSB.

- **Outcome**: Yahoo faced lawsuits and was fined by the SEC. The company's acquisition by Verizon was also affected by the breach.

6. The Sony PlayStation Network (PSN) Hack (2011)

- **Overview**: A major cyberattack on Sony's PlayStation Network resulted in the compromise of personal information from over 77 million accounts, including names, addresses, and credit card details.

[43] In re Capital One Consumer Data Sec. Breach Litig. "MDL No. 1:19md2915 (AJT/JF" In re Capital One Consumer Data Sec. Breach Litig., MDL No. 1:19md2915 (AJT/JFA), (E.D. Va. Jun. 25, 2020)

- **Attackers**: The attack was attributed to the hacktivist group "Anonymous" or other groups with similar motives.

- **Outcome**: Sony faced severe criticism for its lack of security measures. It also had to compensate users and faced several lawsuits.

7. The Target Data Breach (2013)[44]

- **Overview**: Hackers gained access to Target's systems during the holiday shopping season, stealing data from 40 million credit and debit card accounts. Later, an additional 70 million customers had their personal information exposed.

- **Attackers**: The attack was carried out by a group of cybercriminals who gained access through a third-party vendor.

- **Outcome**: Target faced lawsuits, including a multi-million dollar settlement. The company also spent hundreds of millions of dollars on security upgrades.

[44] The Target Data Breach (2013)

CHAPTER 4

CYBERCRIME LAWS IN THE EUROPEAN UNION (EU)

4.1 Introduction

The European Union (EU) has developed a robust legal framework for addressing cyber fraud, combining privacy protections, cybersecurity measures, and criminal sanctions. Key legal instruments that help mitigate and prevent cyber fraud include the General Data Protection Regulation (GDPR), the EU Cybersecurity Act (2019), and the EU Directive on Attacks Against Information Systems (2013). Together, these regulations empower individuals, businesses, and law enforcement authorities to address the growing threat of cyber fraud and enhance the EU's overall cybersecurity resilience.

The European Union has various regulations and directives governing cybercrime to curb cybercrime and harmonize law across the member state. Directive on Security of Network and Information Systems (NIS Directive) was adopted in 2016, the NIS Directive establishes measures to improve the cybersecurity resilience of critical infrastructure and essential services. It mandates EU member states to identify critical infrastructure operators and requires them to implement appropriate security measures, report significant incidents, and collaborate on a crossborder level. The NIS Directive was the first ever EU-wide cybersecurity across the European Union and increase the cooperation between the EU member countries[45]

Another main regulation for cybercrime is General Data Protection Regulation (GDPR). It was implemented in 2018, it is a comprehensive data protection regulation that includes provisions related to cybersecurity. It imposes obligations on organizations to ensure the security and confidentiality of personal data. GDPR requires prompt notification of data breaches and grants individual greater control over their personal information. It aims to encourage controllers and processors to follow the protocols, implement data privacy measures and also ensure that data is collected with consent before publicly available.[46]Moreover, Cybersecurity Act was enforced in 2019, it establishes the European Union Agency for Cybersecurity (ENISA) as a permanent agency [47] ENISA is tasked with enhancing the overall level of cybersecurity in the EU, providing expert advice, and promoting cooperation between member states.

[45] UpGaurd, https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union
[46] Id.

[47] European Commission, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

It will be in charge of informing the public the scheme of certificate and issued certificate through dedicated website.[48] European Cybercrime Centre (EC3) operating under Europol, it plays a crucial role in combating cybercrime. It facilitates information sharing, coordination of cross-border investigations, and supports member states in addressing cyber threats. The main motive is to strengthen the law enforcement response to cybercrime in the EU and thus to protect European citizen, business and the government from any kind of online crimes.[49] EU Cyber Diplomacy Toolbox was adopted in 2017, it outlines the EU's diplomtic response to malicious cyber activities. It includes a range of measures and tools to promote responsible behaviour in cyberspace and to deter and respond to cyber threats. The tool focused to provide instruments to stabilise and secure cyberspace of European Union.[50]

▪ 4.2 General Data Protection Regulation (GDPR)

The GDPR, which came into force in May 2018, is one of the most comprehensive data protection laws in the world. While its primary purpose is to protect the personal data and privacy of EU citizens, it also plays a critical role in preventing cyber fraud by mandating robust safeguards for data security and establishing clear rights for individuals. The key provisions of the GDPR are:

1. **Notification of a Personal Data Breach to the Supervisory Authority (Article 33):** This article mandates that organizations report personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach. A data breach is any incident leading to unauthorized access to, disclosure of, or loss of personal data. For cyber fraud prevention, this means that organizations must promptly alert regulators if a breach occurs, ensuring that malicious actors exploiting vulnerabilities (e.g., hackers or fraudsters) are identified and investigated quickly.

2. **Communication of a Personal Data Breach to the Data Subject (Article 34):** When a data breach is likely to result in a high risk to the rights and freedoms of individuals (e.g., exposure of sensitive financial or identity data), the organization is also required to notify affected individuals without undue delay.

[48] Id.
[49] Europol, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[50] CCDCOE,https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacytoolbox-in-action/#footnote_0_4337

This empowers consumers to take precautionary measures, such as freezing accounts or changing passwords, to mitigate the risk of fraud.

3. **Empowering Individuals to Prevent the Misuse of Personal Data:** The GDPR also provides several rights to individuals that directly help prevent the misuse of their personal data, which is often a primary tool in cyber fraud. These rights include:

4. **Right to Access (Article 15):** Individuals have the right to obtain confirmation from organizations on whether their personal data is being processed. This allows individuals to ensure that their data is not being used fraudulently.

5. **Right to Rectification (Article 16):** If personal data is inaccurate, individuals can request that it be corrected, preventing fraudsters from exploiting incorrect information.

6. **Right to Erasure (Article 17):** Also known as the "right to be forgotten," this right allows individuals to request the deletion of personal data when it is no longer necessary for the purposes for which it was collected, or when it has been unlawfully processed. This provision is particularly useful in preventing fraud that relies on outdated or unnecessary data.

4.3 EU Cybersecurity Act (2019)

The EU Cybersecurity Act (Regulation (EU) 2019/881) was adopted to strengthen the EU's cybersecurity capabilities and provide a unified approach to tackling cyber threats, including cyber fraud. It lays the foundation for a European Cybersecurity Certification Framework, improving the security of products, services, and processes across the EU. This Act plays a central role in enhancing the EU's ability to prevent and respond to cyber fraud by:

1. **Creating the European Cybersecurity Agency (ENISA):** The act strengthens ENISA by giving it a more central role in coordinating cybersecurity efforts across EU member states. This enables the agency to better support national governments in dealing with cyber fraud, share best practices, and provide cybersecurity expertise.

2. **Cybersecurity Certification:** The act establishes an EU-wide cybersecurity certification framework for products and services, which helps ensure that companies meet high security standards, reducing vulnerabilities that fraudsters could exploit. For example, cybersecurity certification of financial platforms or digital payment systems ensures that they are secure against fraud and other cyberattacks.

3. **EU Cybersecurity Risk Management:** The act also introduces requirements for critical sectors (e.g., finance, energy, healthcare) to adopt comprehensive risk management practices and report serious incidents. These measures ensure that organizations are better prepared to prevent cyber fraud by strengthening their defenses against potential attacks.

4.4 EU Directive on Attacks Against Information Systems (2013)

The EU Directive on Attacks Against Information Systems (Directive 2013/40/EU) criminalizes a range of cybercrimes, including those related to cyber fraud. It is one of the most important pieces of legislation in the EU aimed specifically at tackling cybercrime and fraud in the digital age. The directive sets out common minimum standards for the criminalization of attacks against information systems, which is particularly relevant in the context of cyber fraud. It targets activities such as:

- **Hacking:** Unauthorized access to computer systems to steal or alter data for fraudulent purposes.
- **Phishing:** Deceptive practices where fraudsters impersonate legitimate organizations to trick individuals into revealing sensitive personal data (e.g., banking credentials).
- **Denial of Service (DoS) Attacks**: Disabling websites or online services to create opportunities for fraud, extortion, or other malicious activities.
- **Malware and Ransomware:** Distributing malicious software to steal information or hold systems hostage for financial gain.

4.5 Case laws

EU case law regarding cybercrime is primarily centered around the application and interpretation of EU regulations, directives, and frameworks aimed at combating cybercrime. Some significant cases address issues like data protection, cross-border access to data, cybercrime penalties, and the application of EU law to new technologies.

Here are a few key cases related to cybercrime in the EU:

1. Sanchez V. France 2023[51]

The European Court of Human Rights (ECHR) ruled that a politician, Julien Sanchez, did not have his freedom of expression violated when he was convicted for failing to promptly remove hateful comments posted by others on his public Facebook page during an election campaign, essentially holding him accountable for not actively moderating third-party comments on his social media platform despite not directly posting the offensive content himself; this decision raised concerns about potential over-censorship and the potential for users to be held liable for comments posted by others on their social media pages.

Key points about the case:

Context:

Sanchez, a French politician, was running for election and posted a message on Facebook about a political opponent, which led to several users posting hateful comments targeting Muslims on his page.

The ruling:

The ECHR found that Sanchez's failure to remove these comments quickly enough, given the context of an election campaign and the inflammatory nature of the comments, constituted a violation of hate speech laws and was not protected by freedom of expression.

Concerns raised:

[51] Sanchez v. France [GC] - 45581/15

Critics argue that this decision could discourage open online discussion and potentially force social media users to actively monitor and remove all potentially harmful comments posted by others on their pages.

2. The Google Spain Case (C-131/12)[52]

Court of Justice of the European Union (CJEU) – 2014

This case isn't directly about cybercrime, but it addresses important data protection issues in the context of the internet and digital technologies, which are crucial for cybercrime law enforcement. The case established the **right to be forgotten**, requiring search engines like Google to remove links to irrelevant or outdated personal information.

Relevance to Cybercrime:

- This ruling has implications for cybercrime, especially regarding online privacy, personal data misuse, and the protection of individuals from harmful content.
- It discusses the balance between freedom of expression and data protection, which is crucial when tackling issues like defamation, cyberbullying, and online harassment.

3. The "Max Schrems" Cases (C-362/14, C-311/18)[53] CJEU – 2015, 2020

While the Schrems cases (C-362/14 and C-311/18) were focused on data protection and privacy law, they are pivotal in discussions about cybercrime as they address the mechanisms for cross-border data transfer, particularly between the EU and the US.

Relevance to Cybercrime:

- Cybercrime often involves cross-border data flows, and these cases highlight the EU's stance on data protection when dealing with law enforcement agencies, including the sharing of data in cybercrime investigations.

[52] The Google Spain Case (C-131/12)

[53] The "Max Schrems" Cases (C-362/14, C-311/18)

- The ruling invalidated the **Safe Harbor Agreement** and later the **Privacy Shield Agreement**, which had implications for how cybercrime data is handled across borders.

4. The "Digital Rights Ireland" Case (C-293/12)[54] CJEU – 2014

This case focused on the legality of the EU Data Retention Directive, which required telecom operators to retain data for up to two years. The Court ruled that the directive violated fundamental rights to privacy and data protection and declared it invalid.

Relevance to Cybercrime:

- Data retention is often an essential tool in investigating cybercrime. The invalidation of the directive required new frameworks to be put in place to balance law enforcement needs with privacy rights.

- This decision influenced the design of EU cybercrime legislation, particularly in how personal data should be handled in criminal investigations.

5. Case C-291/12 (Schrems II)[55] CJEU – 2020

Schrems II revisited the legal basis for transferring personal data from the EU to the US. The ruling invalidated the EU-US Privacy Shield, which was important for data transfers between jurisdictions. The court emphasized that EU citizens' data rights should not be compromised, particularly when governments have access to data for surveillance purposes.

Relevance to Cybercrime:

- This decision impacts cross-border law enforcement cooperation, a central issue in tackling cybercrime. Data transfers are frequently used in international cybercrime

[54] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others. C-293/12 and C-594-12, ECLI:EU:C:2014:238

[55] Schrems II Case C-291/12

investigations, and the ruling affects how the EU approaches data sharing in cases of cybercrime and other criminal investigations.

6. The "Lautsi v. Italy" Case (C-508/04)[56] European Court of Human Rights – 2011

Although not directly about cybercrime, this case involving the display of religious symbols in public schools touches on broader concepts of human rights in a digital context, especially as issues like hate speech or harmful content online intersect with religious and cultural matters.

7. The Directive on Attacks Against Information Systems (2013/40/EU)

This Directive requires Member States to criminalize illegal access, interference, and data theft in information systems. It aims to harmonize the legal framework across the EU regarding cybercrime, including establishing penalties and procedures for dealing with cyber-attacks and hacking.

Relevance to Cybercrime:

- This legal framework is crucial in addressing cybercrime cases like hacking, malware, ransomware attacks, and other forms of cyber intrusions that affect EU citizens and businesses.

8. The Directive on Cybersecurity (EU) 2016/1148

Also known as the NIS Directive (Network and Information Systems Directive), this piece of legislation aims to improve cybersecurity across the EU. While it's primarily focused on infrastructure and network security, it plays a key role in preventing and investigating cybercrime.

Relevance to Cybercrime:

- It establishes requirements for the security of critical infrastructure, which is increasingly targeted by cybercriminals. It provides a framework for cooperation

[56] The "Lautsi v. Italy" Case (C-508/04)

and information exchange between Member States, which is essential for handling cross-border cybercrime.

9. Case C-74/14 (Pawel S., 2015)[57]

CJEU – 2015

This case deals with the application of criminal law in cross-border cybercrime cases, particularly involving data stored in one EU Member State but accessed or manipulated by users in another. The Court of Justice affirmed that the law of the country where the data is accessed or manipulated can apply in such cases.

Relevance to Cybercrime:

- The ruling underscores the complexity of jurisdictional issues in cybercrime cases, particularly when crimes take place across multiple jurisdictions in the digital space.

10. Case C-136/17 (Weltimmo S.R.O.)[58] CJEU – 2018

The case concerns the application of GDPR (General Data Protection Regulation) and the obligations of companies operating within the EU concerning personal data processing and retention. This is important in tackling cybercrime as data breaches and mishandling of personal data often form the basis of cybercriminal activities.

Relevance to Cybercrime:

- Breaches of data security and mishandling of personal information are often at the heart of cybercrime cases. The ruling in this case emphasizes the need for stringent safeguards for personal data to prevent misuse by cybercriminals.

[57] . Case C-74/14 (Pawel S., 2015)

[58] . Case C-136/17 (Weltimmo S.R.O.)

CHAPTER 5

COMPARATIVE ANALYSIS OF CYBERCRIME LAWS IN INDIA, THE USA, AND THE EU

5.1 Introduction

With the swift development in innovation and growing dependency on technical gadgets, cyber frauds are becoming common rampantly. Technology has entirely dominated the lives of people, which has led to some serious repercussions. Crimes of all kinds are perpetrated online. Due to free flow of information in the cyberspace,

countries are becoming more vigilant regarding data protection as a part of national defense and public welfare. By developing and putting into practice the cyber security policies and proper procedures, the associated risk with cyber crime can be mitigated to certain extent. Privacy and data protection are important issues in all three nations, although the details differ. It is time for all states to develop and enforce comprehensive legal and regulatory frameworks that address cyberterrorism, including laws related to cybercrime, data protection, information sharing, and critical infrastructure protection The Data Protection Act of the United Kingdom is in line with European norms and underscores the significance of protecting personal data[59]

5.2 Analysis

The notice may be sent by registered post acknowledgement due or by speed post or courier or by any other means of transmission of documents like fax message or electronic mail service.

India's legal framework for addressing cybercrime primarily revolves around the Information Technology Act, 2000 (amended in 2008). The act criminalizes unauthorized access, hacking, and the transmission of obscene or offensive content online. The establishment of the Indian Computer Emergency Response Team (CERT-In) further strengthens the country's cybersecurity infrastructure. India also recognizes the importance of international cooperation and has signed agreements with various countries to facilitate the exchange of information in cybercrime investigations.

When it comes to the United States, cybercrime laws are diverse and often overlap between federal and state jurisdictions. The Computer Fraud and Abuse Act (CFAA) is a key piece of legislation that criminalizes unauthorized access, hacking, and related activities. Additionally, the USA PATRIOT Act and the Cybersecurity Information

[59] Federal Laws Relating to Cyber security: Overview of Major Issues, Current Laws, and Proposed

Legislation, available at, https://fas.org/sgp/crs/natsec

Sharing Act (CISA) provide tools for intelligence agencies and private entities to share information on cybersecurity threats.

The Federal Trade Commission (FTC) plays a role in enforcing consumer protection in the digital space. The European Union has a comprehensive approach to cybercrime, with directives and regulations that aim to enhance cybersecurity across member states. [60]The Directive on Security of Network and Information Systems (NIS Directive) focuses on critical infrastructure, mandating measures to ensure cybersecurity resilience. The General Data Protection Regulation (GDPR) is a landmark regulation protecting individuals' data and imposing strict penalties for data breaches. Europol and the European Cybercrime Centre (EC3) facilitate

cross-border collaboration, while the Cybersecurity Act establishes the European Union Agency for Cybersecurity (ENISA). In each country, the definition and scope of cybercrime offenses may vary as per country needs and the environment. Overall, the main motive to have cybercrime law is to tackle the crimes in cyberspace and provide a healthy and safe atmosphere in the digital space. In India, the cybercrime law is revolving on IT Act 2000 as it the primary law regulating cybercrimes.[61]

But when it comes to USA and EU, they have a comprehensive law to regulate cybercrime. Both these countries having specific cybercrime laws to regulate unlike in India. When it comes to data protection, EU is having a strong law which is General Data Protection Centre (GDPR) as compared to USA and India. When it comes to the enforcement mechanism of cybercrimes, USA involves the combination of federal and state agencies including FBI (Federal Bureau of Investigation), Department of Justice which prosecute and provide legal assistance nationwide.

The enforcement mechanism in EU is having a multi-layered approach which includes Europol, European Cybercrime centre and in India, Indian Computer Emergency Response Team (Certin) serves national agency for regulating cybercrimes. When it comes to the penalty, these countries mainly focus on fines and imprisonment. But EU has gone one step ahead by providing hefty penalty for the violation of the same. Overall, these countries laws in regulating cybercrime have similarities. However, differences exit in their legislative framework, enforcement mechanism and regulatory

[60]CCDCOE,https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacytoolbox-in-action/#footnote_0_4337

[61]Europol, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

approach. IT Act in India is acting as a national level whereas in USA, it is the mixage of both federal and state laws in regulating cybercrimes and in European Union having a centralized approach which regulate the member states

5.3 Analysis of legal frameworks in India, the USA, and the EU

This comparative analysis will evaluate the legal frameworks in these three jurisdictions in terms of scope, enforcement mechanisms, technological integration, jurisdictional issues, international cooperation, and the balance between privacy and security.

1. Scope and Coverage:

- India: India's legal framework for cyber fraud is evolving, with cybercrime and data protection laws being progressively updated. Initially governed by the Information Technology Act, 2000 (IT Act), which criminalizes cyber fraud, the framework was updated with the Digital Personal Data Protection Act, 2023 (DPDPA). The IT Act addresses offenses like hacking, identity theft, and data breaches, but it lacks provisions for newer forms of cyber fraud, such as fraud involving cryptocurrencies or AI-driven scams. The DPDPA, enacted in 2023, aims to modernize India's data protection regime by introducing more stringent measures for handling personal data. It enhances the regulatory framework for data breaches, including stronger obligations for data controllers to secure data and notify data subjects in case of breaches. However, India's cybercrime laws still face challenges in keeping up with the increasingly sophisticated nature of cyber fraud.

- United States: The US boasts a comprehensive framework for cyber fraud, particularly through laws like the Computer Fraud and Abuse Act (CFAA), the Identity Theft and Assumption Deterrence Act (1998), and various sector- specific regulations (e.g., HIPAA for healthcare fraud). These laws cover a wide array of cyber fraud activities, from hacking and phishing to identity theft and fraud through financial systems. Despite its robust regulatory landscape, the US suffers from a fragmented approach, as federal, state, and sector-specific laws sometimes lead to overlaps or gaps in enforcement.

- European Union: The EU has developed a unified, multi-faceted legal framework, with core regulations such as the General Data Protection Regulation (GDPR), the EU Cybersecurity Act (2019), and the EU Directive

on Attacks Against Information Systems (2013). The GDPR addresses data protection and security breaches, while the Cybersecurity Act strengthens the EU's cybersecurity framework by certifying critical infrastructure and digital products. This integrated approach makes the EU's framework one of the most comprehensive, particularly in balancing privacy protections with fraud prevention.

2. Enforcement Mechanisms:

- India: Enforcement in India is still evolving. While the Cyber Crime Cells exist at both the state and national levels, they face challenges in terms of capacity, resources, and training. The judicial system is slow in addressing cybercrime cases, and public awareness about how to report cyber fraud remains limited.

- United States: The US has specialized agencies like the Federal Bureau of Investigation (FBI) and Secret Service, which are highly effective in investigating and prosecuting cyber fraud. Additionally, the Federal Trade Commission (FTC) plays a significant role in protecting consumers from identity theft and financial fraud. However, coordination between federal, state, and local authorities can sometimes be a bottleneck in addressing multi- state or multi-jurisdictional cyber fraud cases.

- European Union: The EU benefits from a strong enforcement framework, primarily through Europol and its European Cybercrime Centre (EC3), which coordinate cross-border investigations. National law enforcement agencies are well-equipped to handle cyber fraud, but enforcement can sometimes be delayed due to differing legal standards across member states. The GDPR enforcement is also handled by national Data Protection Authorities (DPAs), but enforcement can vary depending on the country's commitment to compliance.

3. Technological Integration in Legal Responses:

- India: India's law enforcement agencies are still catching up in terms of integrating digital forensics into cyber fraud investigations. While there are some cyber labs in the country, the use of AI and machine learning (ML) is

not widespread. The Cyber Crime Cells use traditional forensic methods, which are often slow and insufficient for handling modern, complex cyber frauds.

- United States: The US is a leader in integrating AI, machine learning, and digital forensics into cyber fraud detection and prevention. The FBI uses advanced AI tools to track down cybercriminals, and financial institutions employ AI-driven systems to detect fraudulent transactions in real time. The private sector also plays a key role in innovating fraud prevention technologies.

- European Union: The EU has also made significant strides in incorporating AI and ML into fraud detection, especially through the Cybersecurity Act and efforts coordinated by Europol. The EU emphasizes ethical considerations in the use of AI for fraud prevention, particularly in relation to GDPR's privacy concerns.

4. Jurisdictional Issues and International Cooperation:

- India: India is a signatory to the Budapest Convention on Cybercrime, which facilitates international cooperation in cybercrime cases. However, India's capacity to effectively engage in cross-border cyber fraud prosecutions is limited by gaps in its enforcement mechanisms and slow judicial processes. The DPDPA addresses cross-border data flows but is still un-tested in addressing jurisdictional issues in cybercrime.

- United States: The US has a well-established framework for cross-border cooperation in cyber fraud cases, facilitated through the Budapest Convention, Interpol, and other international agreements. However, differences in legal frameworks and enforcement practices between countries can create barriers in pursuing international cyber fraud cases.

- European Union: The EU's framework for cross-border cybercrime is robust, with Europol and national authorities collaborating effectively through Mutual Legal Assistance Treaties (MLATs) and other tools. The EU's single market and cohesive legal structure enhance its ability to prosecute cross-border cyber fraud.

5. Privacy vs. Security:

- India: India's privacy laws have been evolving, with the Digital Personal Data Protection Act, 2023 (DPDPA) setting new standards for personal data protection. While the DPDPA focuses on strengthening data security, it also permits certain data processing for law enforcement purposes, which may raise concerns regarding the privacy-security balance.

- United States: The US prioritizes security over privacy in its approach to cyber fraud. Laws like the CFAA allow extensive data surveillance, often for security purposes, but this can lead to concerns about civil liberties and the potential for overreach in the name of fraud prevention.

- European Union: The GDPR is at the forefront of privacy protection, but it also allows for the processing of personal data for purposes of fraud detection and prevention, provided that it complies with strict safeguards. The EU emphasizes the importance of maintaining individual privacy while also ensuring that data can be used to prevent cyber fraud.

5.4 Simplified Comparison of Cybercrime Laws in India, the USA, and the European Union in table below

Aspects	India	USA	European Union
Key Legislation	Information Technology Act, 2000 (amended in 2008)	Computer Fraud and Abuse Act (CFAA), PATRIOT Act, CISA	NIS Directive, GDPR, Cybersecurity Act
Data Protection	Yes (Digital Personal Data Protection Act (DPDP Act)	Yes (Various sector specific laws, e.g., HIPAA)	Yes (General Data Protection Regulation - GDPR)
Agencies	CERT-In	FTC, FBI, DHS, CIA, NSA	Europol, ENISA, National Cyber Security Agencies

International Collaboration	Yes (Bilateral agreements with various countries)	Yes (Information sharing with allied countries)	Yes (Europol, collaborative efforts through ENISA)
Enforcement	Judicial system, law enforcement agencies	Department of Justice, FBI, FTC	National law enforcement, Europol
Focus on Critical Infrastructure	Limited focus	Sector-specific regulations (CISA)	NIS Directive mandates protection of critical infra
Penalties for Data Breaches	Limited as of now, Personal Data Protection Bill	Significant fines, legal actions under CFAA	GDPR imposes hefty fines for data breaches
Approach to Cyber security	Evolving strategies, emphasis on international coop	Varied approaches, public-private partnerships	Comprehensive legal frameworks and cooperation
Scope of Offenses	Unauthorized access, hacking, online offenses	Unauthorized access, hacking, cyber espionage	Unauthorized access, data breaches, cyber threats

CHAPTER 6

INTERNATIONAL COOPERATION IN CYBERCRIME

6.1 Introduction

Cyber crime and terrorism is an international problem which does not respect national borders. Cyber criminals operate from relatively safe territories beyond the easy reach of the law enforcement agencies of the countries in which their victims reside. Collaboration between governments, intelligence agencies and law enforcement officers is critical to prosecuting cybercrime, and new organizations have been created to enable this. However, this co-operation seems to have run into roadblocks by the leak of large scale national level data snooping secrets by whistleblower Edward Snowden. The paper attempts to derive insights from ongoing initiatives reported in open source and recommend options available to charter the path for sustainable international cooperation in evolving secure cyber infrastructure.

Criminals take advantage of this online transformation to target weaknesses in online systems, networks and infrastructure. There is a massive economic and social impact on governments, businesses and individuals worldwide.

Phishing, ransomware and data breaches are just a few examples of current cyberthreats, while new types of cybercrime are emerging all the time. Cybercriminals are increasingly agile and organized – exploiting new technologies, tailoring their attacks and cooperating in new ways.

Cybercrimes know no national borders. Criminals, victims and technical infrastructure span multiple jurisdictions, bringing many challenges to investigations and prosecutions.

Close collaboration between public and private partners is therefore essential. INTERPOL, with its global reach, plays a vital role in building cross-sector partnerships and enabling international law enforcement cooperation.

At INTERPOL, we coordinate law enforcement operations, and deliver secure data sharing platforms, analysis and training in order to reduce cyber threats. By increasing the capacity of our member countries to prevent, detect, investigate and disrupt cybercrimes, we can help protect communities for a safer world.[62]

[62] M. Chaturvedi, A. Unal, P. Aggarwal, S. Bahl and S. Malik, "International cooperation in cyber space to combat cyber crime and terrorism," 2014 IEEE Conference on Norbert Wiener in the 21st Century

(21CW), Boston, MA, USA, 2014, pp. 1-4, doi: 10.1109/NORBERT.2014.6893915.

6.2 UN Cybercrime Convention

On 24 December 2024, the United Nations General Assembly (UNGA) adopted the UN Convention against Cybercrime, marking a significant milestone in the global fight against cybercrime. This treaty, the first legally binding UN instrument addressing cyber issues, establishes a crucial framework for international cooperation in the prevention, investigation and prosecution of cybercrimes. As cyber threats grow in scale and complexity, the convention aims to prevent and combat cybercrime, enhance international cooperation and promote technical assistance and capacity-building, particularly for developing countries. The Convention will be open for signature at a formal ceremony in Hanoi, Vietnam in 2025, and will enter into force 90 days after ratification by the 40th signatory.

The adoption of the Convention underscores the ability of multilateralism to navigate complex global challenges. It also reflects the collective determination of UN Member States to strengthen global cooperation in combating cybercrime. However, the treaty has faced criticism from human rights groups and privacy advocates who warn it could be misused by authoritarian regimes to justify surveillance, monitor citizens' online activities and censor speech under the guise of combating cybercrime.Critics are concerned that the treaty's broad provisions, particularly around data sharing and cross- border law enforcement, could undermine privacy, freedom of expression and be used for political repression. This Brief explores the treaty's potential to shape digital governance while examining the criticisms surrounding its implementation and impact.[63]

6.2.1 Key Features of the UN Convention

The UN Convention aims to enhance the prevention and effective combating of cybercrime, strengthen international cooperation and support technical assistance and capacity-building, particularly for developing countries. It comprises nine chapters: General Provisions, Criminalization, Jurisdiction, Procedural Measures and Law Enforcement, International Cooperation, Preventive Measures, Technical Assistance and Information Exchange, Mechanism of Implementation and Final Provisions.

The chapter on General Provisions addresses the statement of purpose, definitions, scope and key issues such as the protection of sovereignty and the respect for human rights.

[63] "UN General Assembly Adopts Milestone Cybercrime Treaty", United Nations, 24 December 2024.

The second chapter examines the Conventon's role in establishing a comprehensive framework to combat cybercrimes, including hacking, online fraud and child exploitation, with a particular emphasis on cross-border cooperation and capacity-building. A key provision in the criminalization chapter addresses child abuse, encompassing offenses such as online child sexual abuse, the distribution of exploitation material and the solicitation or grooming of a child for the purpose o committing a sexual offence. It underscores the requirement to criminalise cyber-dependent offenses, such as unauthorised hacking and data interference, alongside cyber-enabled crimes, including online fraud and the non-consensual dissemination of intimate images. Furthermore, it addresses the accountability of legal entities while ensuring procedural safeguards for accused individuals

Given the transnational nature of cybercrime, the Convention establishes jurisdictional rules to prevent criminals from exploiting legal gaps. States must claim jurisdiction over offences committed on their territory or affecting their nationals, with provisions for action against offenders within their borders if extradition is not possible. When jurisdictions overlap, States are required to consult with each other. The Convention also mandates cooperation in investigations, including extradition, evidence sharing and mutual legal assistance for electronic data. However, States may refuse cooperation on grounds of sovereignty, public order or non-compliance with data protection or anti- discrimination principles.[64]

The chapter on procedural measures equips States with tools to effectively secure and collect electronic evidence, adapting traditional methods to the ICT environment while protecting human rights. It empowers States to preserve, search, seize and produce electronic data, as well as intercept data in transit, to combat cybercrimes efficiently. These powers are governed by safeguards such as judicial oversight, clear justifications, limited scope and access to remedies, ensuring evidence interity and the protection of rights.

The Convention also establishes a global framework to assist in investigations, prosecutions and judicial proceedings, including extradition, joint investigations and asset recovery. It facilitates cross-border access to electronic evidence through measures like data preservation, access and interception, supported by a 24/7 contact point network for

[64] Article 1, "Draft United Nations Convention Against Cybercrime", United Nations, 9 August 2024

rapid response. It outlines the general principles and procedures for mutual legal assistance, stating that States Parties shall provide each other with the widest possible support in investigations, prosecutions and judicial proceedings. The provisions on international cooperation require States to work closely together, in line with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement in combating these offences.[65]

The Convention promotes collaboration between law enforcement and stakeholders, public awareness campaigns, training for justice officials and the use of security researchers' expertise. It emphasises protecting vulnerable groups, preventing gender- based violence, safeguarding children and supporting victims and offender reintegration. States are required to evaluate their legal frameworks, ensure accessible reporting mechanisms and designate authorities for international preventive collaboration, creating a global network to address evolving cybercrime threats.

The chapter on technical assistance and information exchange focuses on strengthening global capacity to combat cybercrime, particularly in developing countries. It emphasises sharing knowledge and resources for preventing, detecting, investigating and prosecuting cybercrime, including handling electronic evidence, forensic analysis and tracking cybercrime proceeds.[66]

The Convention emphasises providing financial and technical assistance to developing countries to help them prevent and combat the offences covered. States Parties are encouraged to make regular voluntary contributions to a United Nations funding mechanism to support the implementation of the Convention in these countries.The chapter also fosters partnerships between governments, NGOs, academia, financial institutions and the private sector to address the growing threat of cybercrime.

The chapter on the Mechanism of Implementation establishes the Conference of States Parties, responsible for overseeing the Convention's implementation. States parties must submit reports on their implementation measures for periodic reviews, with the Conference offering recommendations to improve effectiveness.29 The Conference facilitates information exchange on legal, policy and technological developments, and may adopt supplementary protocols. It can also collaborate with stakeholders, including

[65] Ibid., Articles 28, 29 and 30.
[66] Ibid., Article 53 (3) h & i.

international organisations, NGOs and the private sector. The first Conference will be convened by the UN Secretary-General within a year of the Convention's entry into force, with the United Nations Office on Drugs and Crime (UNODC) serving as its secretariat.

The chapter on final provisions outlines the procedures for States to become parties to or withdraw from the Convention, as well as the rules governing its entry into force and its legal effects. It also covers the settlement of disputes related to the interpretation or application of the Convention, emphasising that such disputes should be resolved primarily through negotiations or other peaceful means, including arbitration. If necessary, the International Court of Justice may be called upon to settle disputes at the request of the parties involved. Furthermore, the chapter provides for the potential amendment of the Convention and the addition of supplementary protocols. States may withdraw from the Convention through written denunciation, with the withdrawal taking effect one year after the notification is made.

6.2.2 Contrasting the UN and Budapest Conventions

The Budapest Convention on Cybercrime, adopted in 2001, was the first international treaty focused on combating cybercrime and strengthening cross-border cooperation. While both the Budapest and UN Conventions seek to combat cybercrime, their scopes differ significantly. [67]The Budapest Convention focuses on criminalising specific offences, establishing procedural measures and facilitating cross-border access to electronic evidence.33 In contrast, the UN Convention adopts a broader approach, emphasising prevention, capacity-building and technical assistance, with particular attention to supporting developing countries. Additionally, the UN Convention offers a global framework for cooperation on serious cybercrimes and incorporates provisions related to state sovereignty and prevention, expanding its scope beyond the Budapest Convention's emphasis on criminalisation and procedural mechanisms.[68]

The definitions in the UN Convention largely align with those in the Budapest Convention, with key differences that reflect the broader scope of the UN Convention.

[67] "The New UN Cybercrime Treaty is a Bigger Deal Than Even Its Critics Realize", Lawfare, 2 October 2024.
[68] "Comparative Analysis: The Budapest Convention vs the UN Convention Against Cybercrime", digwatch, 22 October 2024.

Notably, the UN Convention adopts the terms "ICT" and "ICT systems" instead of the "computer" and "computer systems" terminology used in the Budapest Convention, reflecting the evolving nature of technology and the increasing reliance on information and communication technologies.

While both conventions criminalise offences such as illegal access to systems, the UN Convention extends its focus to include additional crimes, such as money laundering, and places greater emphasis on child sexual abuse. For example, while the Budapest Convention criminalises the possession and distribution of child abuse material, the UN Convention also targets preparatory offences, including grooming and solicitation, thus broadening its approach to combating such crimes. Furthermore, the procedural powers in the UN Convention are broader than those in the Budapest Convention. For instance, the UN Convention includes measures for the confiscation of proceeds from crime and the protection of witnesses, which are not addressed in the Budapest Convention.[69]

6.3 NPA INTERPOL Asia and South Pacific Joint Operations on Cybercrime (ASPJOC)

Strengthening the capability of Asian and South Pacific law enforcement agencies to fight cybercrime Duration: 1 June 2024 – 31 March 2025 (Phase 1)

Beneficiary member countries: Brunei, Cambodia, Fiji, Indonesia, Kiribati, Laos, Malaysia,Marshall Islands, Nauru, Papua New Guinea, Philippines, Samoa, Singapore, Solomon Islands, Thailand, Timor-Leste, Tonga, Vanuatu and Vietnam.

Donor: The United Kingdom Foreign, Commonwealth & Development Office

Project aim

ASPJOC aims to strengthen the capability of Asian and South Pacific (ASP) national law enforcement agencies to prevent, detect, investigate, and disrupt cybercrime by:

- Gathering and analyzing information on cybercriminal activity;
- Promoting cooperation and good practices amongst asia and south pacific member countries;

[69] Ibid., Article 33.

• Facilitating and carrying out intelligence-led, coordinated action against cybercrime.

Project activities

INTERPOL supports member countries in the fight against cybercrime in four core areas of work:

1. Analytical support and threat intelligence

Publishing and disseminating cyber threat assessments, advisories, and activity reports to equip ASP member countries with insights into the region's latest cyber threats and trends for resource prioritization and strategic decision-making

2. Awareness-raising campaigns

Providing practical guidance for detecting pertinent cyber threats, supporting law enforcement prevention efforts for improved operational outcomes, and promoting good cyber practices for individuals and organizations in the ASP region.

3. Joint operational framework and working group meetings

Establishing mechanisms and platforms for secure and effective information sharing between ASP law-enforcement agencies, other intergovernmental organizations, and private sector partners in countering cybercrime.

4. Investigative assistance and operational coordination

Driving intelligence-led operations, coordinated actions, and disruption efforts against cybercrime, related infrastructure, and its perpetrators operating in or affecting Asia and the South Pacific.

We also work in close partnerships with relevant regional stakeholders, the private sector, and other key partners to better assist law enforcement authorities in reducing the impact of cybercrime.[70]

6.4 AFJOC - African Joint Operation against Cybercrime

Reinforcing cybersecurity in Africa Timeframe: 2024 to 2025

Budget: GBP 2.68 million

Donor: United Kingdom - Foreign, Commonwealth & Development Office (UK FCDO)

[70] https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/INTERPOL-Asia-and-South-Pacific-Joint-Operations-on-Cybercrime-ASPJOC

The situation

The African region is seeing unprecedented growth and development in the digital technology sector, particularly in financial technology and e-commerce.

However, this rapid digitalization has also brought with it a variety of security threats that can have a severe impact. Leveraging the increased reliance on technology, attackers employ various techniques to steal personal data and execute fraudulent activities. Prominent cyber threats in the region include digital extortion, ransomware deployments, sophisticated online scams (like phishing), and business email compromise (BEC) schemes.

The absence of robust cybersecurity standards creates a critical gap in protecting online services. This exposes critical infrastructure like banks and government institutions to cyberattacks, potentially leading to data breaches, financial losses, and disruptions in trade. Addressing this gap through stronger cybersecurity standards is essential.

Project aims

Building upon the achievements of the AFJOC initiative (2021-2023), the AFJOC II project aims to further enhance the capabilities of national law enforcement agencies in Africa. This will be achieved through continued focus on preventing, detecting, investigating, and disrupting cybercrime activities. This is achieved by:

Gathering and analysing information on cybercriminal activity;

- **Carrying out intelligence-led, coordinated action;**
- **Promoting cooperation and best practice amongst African member countries.**

Project activities

Analytical support and intelligence – timely and accurate intelligence is vital in any effective law enforcement response to cybercrime. Our Cyber Activity Reports are important resources, providing insight on cyber threats targeting specific countries or regions;

Developing regional capacity and capabilities to combat cybercrime – collaborative platforms such as the Cybercrime Collaborative Platform and Cyber Fusion Platform allow for secure communications and exchange of data on operations;

Joint Operational Framework – this addresses cybercrime threats through collaboration between law-enforcement agencies, private sector and other international/intergovernmental organizations;

Operational support and coordination – our operations help dismantle the criminal networks behind cybercrime;

Awareness-raising campaigns – promoting good cyber practices for individuals and businesses in Africa.

Our African Cybercrime Operations Desk is responsible for implementing AFJOC. It works in close partnership with key regional stakeholders, in particular the African Union and AFRIPOL, law enforcement communities and the private sector

6.5 India international cooperation of cybercrimes

The effective combating of Cybercrimes require international cooperation among countries, law enforcement agencies and institutions backed by laws, international relations, conventions, directives and recommendations to fight Cybercrime. Cooperation among countries to the widest extent possible and efficient mutual legal assistance is the need of the day.

International Cyber Security Workshop

In the workshop, the participating countries discussed about cyber security measures, and cyber exercises were held on growing threat of ransom ware. This event helped to improve each country's counter measures for ransom ware and strengthen relationship among each other. The workshop is hosted by Japan every year since 2018.

India-EU Cyber Dialogue

The Sixth India-EU Cyber Dialogue was hosted in a virtual mode by India on 14th December 2020. Both sides discussed various areas of cooperation in the cyber space

including contemporary matters; multilateral and regional cooperation on stability in cyberspace at UN platforms; Cooperation on Cybercrime and capacity building.

India-France Bilateral Cyber Dialogue

The Fourth India-France Bilateral Cyber Dialogue was held on 13th October 2021. The Cyber Dialogue discussed various aspects of existing bilateral cooperation in cyberspace, exchanged views on the latest developments on cyber issues at bilateral, regional and multilateral fora and explored initiatives to further strengthen cyber cooperation.

Shanghai Cooperation Organisation (SCO)

The National Security Council Secretariat (NSCS), Government of India organized a Practical Seminar from in December on "Securing Cyberspace in the Contemporary Threat Environment" for delegates from Shanghai Cooperation Organisation (SCO) Member States.

Sessions of the Ad Hoc Committee (AHC)

Ad Hoc Committee to elaborate a comprehensive International Convention on Countering the Use of Information and Communications Technologies (ICTs) for criminal purposes, established by the UN General Assembly in its resolution 74/247, held its second session in Vienna, 30 May to 10 June 2022.

Eighth Meeting of the BRICS Working Group

The 8th meeting of the BRICS Working Group was held on 24th May 2022 regarding Security in the use of Information and communication Technology (ICT) in virtual mode.

Sixth India - Germany Bilateral Cyber Dialogue

The 6th India-Germany Bilateral Cyber Dialogue was held in April 2022 in Bonn and Berlin, Germany. Discussions on the latest developments in the national cyber policies and strategies in the areas of cybersecurity were held.

Fifth India - UK Bilateral Cyber Dialogue

India and the UK held their Annual Cyber Dialogue in London on 12th April 2022. Both sides welcomed the substantial bilateral engagement which covered cyber governance,

deterrence and mutual resilience. They reiterated their commitment to a joint programme of action and next steps in implementing the Enhanced Cyber Security Partnership.

Fourth India - Japan Cyber Dialogue

The Fourth India-Japan Cyber Dialogue was hosted by India virtually on 30 June 2022. Both sides discussed important areas of bilateral cyber cooperation and reviewed the progress achieved in the areas of cybersecurity and Information and Communication Technologies (ICTs) including 5G Technology.

Counter Ransomware Initiative

A Counter Ransomware Initiative meet was held in May 2022 to discuss methodologies to counter ransomware, important ransomware incidents in the past and experiences for predictive analysis, governments involvement and role in managing ransomware incident response, and how to incentivize reporting of ransomware incidents among other related issues. India participated as a lead in a Resilience working group in the meet.[71]

[71]https://i4c.mha.gov.in/internationalcooperation.aspx#:~:text=The%20effective%20combating%20of%20Cyber

crimes,and%20recommendations%20to%20fight%20Cybercrime.

CHAPTER 7

EMERGING TRENDS IN CYBERCRIME

7. 1 Introduction

The rapid proliferation of the internet and digital technologies has revolutionized how we live, work, and communicate. However, this digital transformation has also led to a surge in cyber crimes, posing significant challenges for individuals, businesses, and law enforcement agencies in India. In this article, we will explore some of the recent trends in cyber crime in India, providing insights into the evolving landscape of digital threats and the measures being taken to combat them.

The landscape of cyber crime in India is continually evolving, driven by advancements in technology and the increasing digitalization of society. Staying ahead of these threats requires a multi-faceted approach, involving robust cybersecurity measures, stringent laws, public awareness, and international cooperation. As we navigate this digital age, it is crucial for individuals, businesses, and the government to remain vigilant and proactive in safeguarding against cyber threats.[72]

In the current digital era, the frequency and complexity of cyber threats are increasing. It is imperative that individuals and organizations stay up-to-date on the latest Cybersecurity technologies in order to effectively combat these threats and safeguard sensitive data. It is essential to remain vigilant as new threats emerge daily.

Cybercriminals are becoming more sophisticated in their tactics, and as a result, data breaches are becoming increasingly common. Some of the latest Cybersecurity threats include phishing attacks, ransomware, social engineering, and IoT attacks. These malicious activities can cause significant financial losses, reputational damage, and even legal liability.

Staying ahead of the curve in Cybersecurity is crucial for preventing cyberattacks and protecting sensitive data. Adopting the latest Cybersecurity technologies enables organizations to enhance their security posture and mitigate potential risks. By doing so, organizations can safeguard their information and protect themselves from potential threats. In a nutshell, staying current with the latest Cybersecurity technologies is no longer an option, it is a necessity to ensure the safety of sensitive data and the integrity of business operations.

[72] Recent Trends in Cyber Crime in India, Ankesh Singh (2024)

7. 2 Data Privacy and Protection

In this era of globalization and technology, related crimes have also evolved, resulting in the bubbling up of cybercrime. As the name suggests, the crime committed in a cyber or virtual world is defined as cybercrime. There is a plethora of cybercrimes; for instance, fraud with personal identity, banking or financial theft, selling and stealing corporate data, Cryptojacking and Cyberespionage, Ransomware attacks etc.

After the right to privacy was declared as an integral part of Article 21 of the Constitution of India in the case of Justice K.S. Puttaswamy (Retd.) & Anr. Vs Union of India & Ors, this issue gained a lot more limelight. Firstly, the importance of privacy must be interpreted separately to understand the meaning of data privacy. Privacy does not have a well-framed definition, so it can be roughly defined as a person's right to control the usage mechanism of their data. While surfing through the internet, they are not being monitored. Hence, data privacy is a subset of data security that deals with managing data, who is using it, and in what form.

"Cybercrime is a criminal offence on the Web, a criminal offence regarding the Internet, a violation of law on the Internet, an illegality committed with regard to the Internet, breach of law on the Internet, computer crime, contravention through the Web, corruption regarding Internet, disrupting operations through malevolent programs on the Internet, electric crime, sale of contraband on the Internet, stalking victims on the Internet and theft of identity on the Internet."

Cybercrime affects the data privacy of consumers in many ways; distributed denial-of- service (DDoS) attacks are made by the hackers, which bring down the network for a while and in the meantime, the hackers enter into the system for further actions, identity theft is done against the consumer by gaining control over their personal information, it is hazardous as they may perform any criminal act on the name of the consumer, for example, they may hack the password of social media accounts etc., online scams also come under the purview of cybercrime where the promise of rewards and messages of credited amounts are made to the consumer to lure them into it. Phishing is the most common type of cybercrime, where malicious e-mails and attachments are sent to consumers to enter their systems.

The problem in the case of medical genetic data is also quite similar; the information is stored in the DNA banks, also known as genetic databases, which, although they hold several advantages, put up the personal data of individuals at stake. When the data fiduciaries take over this data, it becomes untraceable; hence, individuals do not know the usage and management of their data.[73]

Cybercrime in India is growing continuously. In August 2019, a National Cyber Crime Reporting Portal was initiated by the Ministry of Home Affairs (MHA) to let people report cases of such crimes. The reported instances crossed all the limits, and the count went to more than three lakhs in less than two years. The reports also revealed that people from the cyber hub of the country, especially Maharashtra and Karnataka, were the most victimized.[74]

In another report put forward by Indian Computer Emergency Response Team (CERT-In), it was revealed that "a total number of 1,59,761; 2,46,514 and 2,90,445 cyber security incidents about digital banking were reported during the years 2018, 2019 and 2020 respectively[75]

Anoymization is a technique that can be used. By hashing the unique identifiers of each row, a unique indexing110

G. Ateniese, M. Steiner, and G. Tsudik ," Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE Trans. on Cloud Computing, 2015.

of each row in the database is created. The hashing information must be maintained locally, and the table must be separated by columns to separate cloud providers after these specific identifiers are removed. Person anonymity is preserved in this manner; but, since the whole column would be stored in a single cloud, data mining attacks may be used to anticipate valuable information.

[73] PTI, Parliament proceedings | Over 2.9 lakh cyber security incidents related to digital banking reported in 2020: Dhotre, The Hindu, (Jan 5, 2023) https://www.thehindu.com/sci-tech/technology/over- 29-lakh-cyber-security-incidents-related-to-digital-banking-reported-in-2020/article33757241.ece
[74] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., (2017) 10 SCC 1.

[75] https://www.livelaw.in/columns/cybercrime-a-threat-to-data-privacy-222766

7. 3 Artificial Intelligence (AI) and Machine Learning (ML)

With recent advances in artificial intelligence, the possibility of cyber threats and crimes has increased exponentially. It has been used in almost every scientific and engineering area. AI has revolutionized everything from hospitals to robots. Since cyber criminals couldn't keep this ball of fire from them, "normal" cyber attacks have evolved into "intelligent" cyber attacks

Artificial Intelligence (AI) and Machine Learning (ML): Artificial Intelligence and Machine Learning are revolutionizing the cybersecurity industry. These technologies analyze vast amounts of data, learn from patterns, and make predictions about potential threats. By utilizing these technologies, cybersecurity experts can identify and respond to threats faster and more accurately than ever before.

The majority of machine learning applications rely on data. Developers of machine learning systems use training data to train variations of these algorithms. The paradigm evolves as a result of the preparation. Machine learning is an iterative technique, which entails a continuous process of analyzing these models and adapting training data and learning algorithms to optimize for performance, as described and decided by developers. Machine-learning strategies, as previously said, depend for instructions on what to look for. Feature engineering, or choosing the characteristics the machine-learning algorithm can train, is an important human factor in machine learning.64In reality, this is a much more difficult job for developers than actually performing the learning process. Although attempts to minimize human interference in feature selection are growing, this is impossible[76]

In late May 2018, NITI Aayog and ABB India signed a letter of intent to 'make core sectors of the Indian economy ready for a digitalized future and recognize the promise of AI, big data, and connectivity.'67NITI Aayog's ultimate target for a national AI strategy is to "leverage AI for economic growth, social change, and sustainable growth, and finally as a "Garage" for emerging and developed economies," according to a discussion paper published in June 2018. The task of the NITI Aayog goes beyond simply proposing a policy approach; it also involves execution and deployment. In two aspects, the National Strategy goes beyond and above any other AI policy

[76] Gillespie T. 2014 The relevance of algorithms, Media technologies: essays on communication, materiality and society 167

mechanism.First, it admits that AI implementation has primarily been motivated by business interests to date, and it recognizes the "need to find a balance between limited financial effects concepts and the common good."Second, it recognizes that AI implementations in different sectors should be accepted for their incremental benefit rather than their alleged transformational value.[77]

7. 4 Behavioral Biometrics

Behavioral biometrics is a new approach to cybersecurity that uses machine learning algorithms to analyze user behavior. This technology can detect patterns in the way users interact with devices, such as typing speed, mouse movement, and navigation. By analyzing these patterns, behavioral biometrics can identify potential threats, such as hackers who have gained access to a user's account.

7. 5 Zero Trust Architecture

Zero trust is a security model that requires strict identity verification for every person or device that tries to access an organization's network or resources. This model assumes that no one is trusted by default, even if they are within the organization's network perimeter. Zero trust architecture has gained popularity in recent years due to the increasing number of cyberattacks targeting businesses and organizations.

7. 6 Blockchain

Blockchain technology is most associated with cryptocurrencies, but it has the potential to transform cybersecurity as well. By creating a decentralized database, blockchain can provide secure storage for sensitive information. Because there is no central authority controlling the data, it is much more difficult for hackers to gain unauthorized access

7. 7 Quantum Computing

Quantum computing is a technology that uses quantum mechanics to process data. It has the potential to solve complex problems much faster than traditional computers. While this technology is still in its infancy, it has the potential to revolutionize the field of cybersecurity by allowing more secure encryption.

[77] Gupta K. 2018 NitiAayog partners with Google to grow India's artificial intelligence ecosystem. Livemint. See

https://www.livemint.com/Industry/fpnGnNQ8duTCRZOEpk 2P6M/Niti-Aayog-partners- with-Google-togrow-Indias-artificial-i.html.

7. 8 Cloud Security

Cloud computing has become an essential part of many businesses, but it also introduces new security risks. Cloud security technologies are emerging to address these risks, such as multi-factor authentication, encryption, and access controls. By utilizing these technologies, businesses can ensure that their data is secure in the cloud.

7. 9 Denial of service (DoS) attacks

These attacks involve flooding a computer or website with information, preventing them to function properly. These attacks are aimed to exhaust the resources available to a network, application or service, in order to prevent users from accessing them. They are more frequently aimed at businesses, rather than individuals. Distributed denial-of-service (DDoS) attacks are those attacks in which multiple compromised computers attack a single target. A DoS attack does not usually result in the theft of information or other security loss, but it can cause financial or time loss to the affected organisation or individual, because of its effects (particular network services becoming unavailable, websites ceasing operation, targeted email accounts prevented from receiving legitimate emails, etc.)[78]

Internet of Things (IoT) Security: IoT devices are becoming more prevalent in homes and businesses, and they are often vulnerable to cyberattacks. IoT security technologies include encryption, access controls, and monitoring to protect IoT

[78] https://dig.watch/topics/cybercrime

CHAPTER 8

Conclusion and Recommendations

8.1 CONCLUSION:

The distinct legal, cultural, and technological landscapes of the United States, the European Union, and India are reflected in their respective cyber security legislation. Information technology Act, 2000 and National Cyber Security Policy has made noteworthy efforts to elevate cyber security in India. Still, concerns with allocation of resources, implementation, and the dynamic nature of cyber threats continue to exist. Cyber security dangers are addressed by a comprehensive legal framework in the United States, which includes important laws like the Federal Exchange Data Breach Notification Act and the Cybersecurity Information Sharing Act (CISA). The American strategy places a strong emphasis on sector-specific attention, information sharing, and public-private partnerships. The EU has created a strong legislative framework for cyber security. The legal strategy adopted by the EU demonstrates a dedication to working with foreign partners, enforcing laws, and safeguarding vital infrastructure. Its legal system clearly strikes a compromise between the needs of national security and individual privacy. India, the USA, and the EU share common objectives in addressing cybercrime; the differences in their legal frameworks reflect regional priorities, legal traditions, and approaches to cybersecurity governance. Harmonizing international efforts and sharing best practices remain critical in the global fight against cyber threats. The privacy and data protection are important issues in all three nations, although the details differ. Although every nation has made progress in tackling cyber security issues, several themes come up again and time again: public awareness, international cooperation, and constant adaptability to new threats. These countries must jointly confront the difficulty of striking a balance between the demands of individual privacy rights protection and national security.

The comparative analysis of the legal frameworks in India, the United States, and the European Union highlights both the strengths and weaknesses of each jurisdiction's response to cyber fraud. In India, the introduction of the Digital Personal Data Protection Act, 2023 (DPDPA) represents a significant step towards improving data protection and mitigating cyber fraud. However, it is yet to be tested and its enforcement will remain a challenge due to gaps in infrastructure, legal clarity, and technological capacity. The US legal landscape is more robust in addressing cybercrime, with a strong emphasis on data breach notifications and consumer rights. However, the fragmented nature of US laws

and the challenges posed by varying state laws can create inconsistencies in enforcement. The EU's legal framework, provides a comprehensive and unified approach to data protection and cybersecurity, with a strong focus on cross-border cooperation. However, the complexity of EU regulations may sometimes result in bureaucratic hurdles and enforcement delays.

Across all jurisdictions, a common challenge is the constant evolution of fraud tactics, which outpaces the legislative response. While India and the US are still catching up in terms of technological enforcement mechanisms, the EU benefits from a more coordinated regulatory approach but struggles with maintaining flexibility to adapt to rapidly evolving threats.

8.2 Recommendations for India:

Based on the strengths of the legal frameworks in the US and EU, several improvements can be made to India's legal framework for combating cyber fraud.

- Cross-Border Cooperation: India should enhance its international cooperation mechanisms for tackling cyber fraud. This can be achieved through better integration with global frameworks such as the Budapest Convention on Cybercrime, ensuring easier information sharing, and enhancing cooperation with foreign law enforcement agencies. The EU Cybersecurity Act and the CFAA provide useful models in this regard, with their emphasis on multilateral collaboration in the fight against cybercrime.
- Improved Data Breach Notification Systems: India's DPDPA would benefit from a more explicit and stringent data breach notification system, similar to the CCPA. This would ensure that organizations are legally compelled to notify affected individuals in a timely manner, increasing transparency and accountability. Clear timelines and consequences for non-compliance would further strengthen the framework.
- Digital Forensics and Enforcement Capacity: India should invest in digital forensics capabilities and specialized training for law enforcement. Drawing inspiration from the US's approach, India can improve its technical capacity to handle complex cyber fraud investigations, particularly by establishing dedicated cybercrime units and increasing the use of AI and blockchain in tracing and preventing fraudulent activities.

8.3 There should be Special Cyber Crime Investigation Cell and Cyber Police for Cybercrime

The Cybercrime Investigation Cell works under the Central Bureau of Investigation, it was notified in September, 1999 and started working from March 31, 2000. The cell has the jurisdiction all over India. It has the power to investigate the offenses mentioned in Chapter XI of the IT Act, 2000 and is also empowered to investigate into other cybercrime cases. It has headquarters in Delhi, Mumbai, Chennai, Bangalore, Hyderabad and Kolkata.

Cybercrime police stations have been set up by the State Governments. As per rules, these cells are handled by specially trained police officials assisted by information technology experts as and when needed for the investigation of cybercrimes. But, in reality they are not properly trained nor well equipped with information technology assisted tools and have no adequate cyber forensic experts. The investigators should be empowered to conduct search and access the data or information in private computer systems and computer equipment's etc. with the earlier approval by the magistrate.

Online Courts / E-Judiciary and Video-conferencing should be used for speedy justice To develop an efficient mechanism of cybercrime adjudication, the e- judiciary framework as proposed under the National Policy on Information and Communication Technology ought to be utilized successfully to ensure effective and speedy disposal of cases. The national e-Court project has begun in July, 2007 for the e-judiciary and egovernance network covering India's whole judicial system. This would ensure transparency, speed and fairness in the adjudication of cases. It would likewise lessen responsibility of the courts and will guarantee expedient disposal of cases because of elimination of issues related with paper- based records like collection, maintenance, retention etc. The retrieval and retention of electronic evidence is much easier.

8.4 Need for Cyber Crime Reporter or Cyber Law Journal

The statistics related to crime fails to reflect the true picture of cybercrime. The reason for this is that ability of computer software makes the detection of cybercrime Conclusion and. The victims of cybercrime often refrain from reporting to avoid unnecessary harassment of time money and energy, and more time consuming judicial process. Companies often refrain from reporting cybercrime in fear of loss of goodwill, or fear of adverse publicity or any other detrimental repercussion.

Lack of necessary technical expertise is also contributing factor to non-reporting of cybercrime cases. Crimes committed by unknown criminal makes the problem more serious, because of lack of any idea about the criminal. In cybercrime cases are either dropped due to lack of evidence, or it may be compromised by parties and very few cases reach to a decision by the court. Therefore, it is very important that the cases should be reported and scrutinised. Because the number of cybercrime cases is increasing enormously, therefore, the publication of a Cyber Law Journal' will definitely help from members of the Bar Bench and investigating agencies

8.5 The Future of Cyber Fraud Prevention:

The future of cyber fraud prevention will increasingly depend on the integration of emerging technologies, global cooperation, and evolving legal frameworks. Technologies such as artificial intelligence (AI) and blockchain hold tremendous potential to transform the fight against cyber fraud. AI can assist in detecting anomalies and predicting fraud patterns, while blockchain's decentralized nature could be leveraged to create tamper-proof records for transactions, enhancing transparency and trust.

However, these technologies also present new challenges, including the potential for fraudsters to exploit AI in their schemes or to find ways to circumvent blockchain's security features. Additionally, the rise of quantum computing could eventually undermine the encryption protocols currently used in fraud prevention, demanding a proactive approach from lawmakers and regulators to prepare for such disruptions.

On the global stage, cyber fraud continues to be a cross-border issue that requires strong international coordination. The EU's focus on cooperation through the GDPR and its collaborative approach with international bodies is an example that other countries, including India, can adopt to address the borderless nature of cybercrime. Cross-border jurisdictional issues must be tackled through the establishment of clearer international legal standards, faster extradition processes, and mutual recognition of cybercrime-related evidence.

In conclusion, while the legal frameworks of India, the US, and the EU each offer valuable insights, the fight against cyber fraud requires an evolving, flexible, and technologically-savvy approach. By learning from the best practices of these jurisdictions and preparing for the challenges of emerging technologies, India can build a more robust legal infrastructure to combat cyber fraud effectively and ensure the protection of its citizens in the digital age.

8.6 Suggestion for International perspective

There must be global cyber legislation to deal with cybercrime cases. The cybercriminals often take advantage of vulnerability of computer system and network that is being attacked. Therefore, a special security measure is essential to combat such cybercrime. As suggested by G8 countries in France, in May 2000, the cyber laws must be universalized so as to extend adequate protection to individuals, or organization, government and non-government agencies and ultimately the society at large. There is need to frame uniform definition and classification of various cybercrimes so that uniform criminalisation can be done for effective combating of cybercrimes throughout the world.

A regulatory mechanism should be established to aid investigation and protection from cybercrime. At present, many ransomware attacks and fraud related to Bitcoin (Bitcoin is a type of money that is completely virtual) came into light, which affected the whole world. However, in the absence of any regulatory mechanism at global level, cybercrime is not properly dealt with. Until now, the world could not reach agreement on this subject.

Central Emergency Response Team (CERT) should be more effective to deal with problem of Cyber Terrorism. The working of CERT should be more cooperative

with other security agencies at the national and international level to deal with cyber-terrorism. Its key functions are analysis, collection, and dissemination of information about cyber incidents, assessment and alert of cyber security, take emergency measures and coordination of cyber incidents response activities. Countries have established their own Incident Response and Computer Security Teams to deal with cybercrime, within territorial limits. Such forum needs to be more cooperative at international level to share and exchange information.

Promoting Mutual Legal Assistance Treaty with all countries is also essential to deal with these cases. The Act recognizes the extraterritorial jurisdiction of cyber law, but it cannot be effectively applied in cases where the criminal is from a country with which India has no extradition treaty. This problem can be dealt with by making suitable extradition treaty

8.7 The Need for Universalisation of Cyber Law

In the 21st century, the world has witnessed an unprecedented rise in the use of digital technologies, especially the internet. With this digital boom, our personal, professional, and commercial lives have become deeply intertwined with cyberspace. As more and more people rely on computers and the internet for communication, finance, education, entertainment, and commerce, the threat of cybercrime has also grown significantly. This digital dependency has introduced not just conveniences but also vulnerabilities, exposing individuals and institutions to new and sophisticated forms of criminal activity. In this context, there is an urgent and undeniable need to universalise cyber laws across countries to ensure consistent protection, cooperation, and accountability.

The Expanding Scope of Cybercrime

Cybercrime is no longer limited to simple email fraud or hacking attempts. It encompasses a broad range of malicious activities such as identity theft, cyberstalking, phishing, ransomware attacks, financial fraud, data breaches, online defamation, and terrorism-related activities. Moreover, with the advent of Artificial Intelligence (AI), the Internet of Things (IoT), and 5G technology, cybercrimes have become more targeted, automated, and destructive. Even

everyday devices such as smart TVs, digital assistants, and connected home appliances can be exploited as entry points for cyberattacks.

What makes cybercrime even more complex is its borderless nature. Unlike traditional crimes that are bound by geography, cybercrimes can originate in one country and impact individuals or institutions across the globe. This extraterritorial nature of cybercrime makes jurisdictional enforcement of laws extremely difficult. It often leads to legal loopholes, allowing perpetrators to escape prosecution if cyber laws in their home country are weak, outdated, or non-existent.

Challenges in National Cyber Laws

Most countries today have some form of legislation to regulate cyberspace. However, the nature, strength, and enforcement of these laws vary significantly. Some nations have robust legal frameworks that cover issues like data protection, cyberbullying, online fraud, and digital forensics, while others are still struggling to formulate basic regulations.

A major concern is that many national laws are designed more for protecting the state's security and sovereignty than for addressing the needs of individual users or private corporations. As a result, these laws may overlook essential aspects like user privacy, digital rights, and international cooperation. There is also the challenge of rapid technological evolution, where laws often lag behind new developments in technology, making them obsolete or ineffective.

Need for Harmonization and Global Collaboration

Given the global nature of the internet, cyber laws cannot remain confined within national borders. There is an increasing need for a **universal legal framework** that governs cyber activities, ensures justice for victims across nations, and provides clear procedures for the investigation and prosecution of cybercrimes.

Universalisation of cyber law implies the creation of a common set of rules, definitions, procedures, and penalties that are accepted and implemented by nations worldwide. This would facilitate:

1. **Efficient Cross-Border Investigations:** A harmonised legal framework would make it easier for law enforcement agencies in different countries to cooperate in real-time, share information, and jointly investigate cyber incidents.
2. **Extradition and Prosecution:** With unified laws, it would become easier to extradite cybercriminals from one country to another and prosecute them under universally accepted legal standards.
3. **Protection of Digital Rights:** A global legal system could ensure the protection of fundamental digital rights such as privacy, freedom of expression, and protection from surveillance.
4. **Confidence in Digital Transactions:** Businesses and consumers would have greater confidence in cross-border digital transactions, knowing that there are robust international laws to safeguard them.

Existing Efforts and Their Limitations

Several international efforts have been made to address the issue of cybercrime through treaties and conventions. The **Budapest Convention on Cybercrime (2001)**, initiated by the Council of Europe, is one such example. It is the first and most comprehensive international treaty seeking to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations.

However, the Budapest Convention is not without its shortcomings. Many major cyber powers such as Russia, China, and India have not signed the treaty, citing concerns over sovereignty and control over domestic digital policies. Furthermore, the treaty does not comprehensively cover new threats such as AI-driven cyberattacks or cyberwarfare.

Other regional efforts, such as the **European Union's General Data Protection Regulation (GDPR)** or the African Union's **Convention on Cyber Security and Personal Data Protection**, reflect growing recognition of the need for regulation. Yet, the lack of a **globally accepted, enforceable, and adaptable cyber law** remains a significant barrier.

The Role of Technology Companies and Web Service Providers

The private sector, particularly major tech companies and web service providers, also plays a critical role in maintaining cyber security. These entities often store sensitive user data, provide cloud services, and control major platforms of communication and commerce. They must therefore adopt stringent security protocols and exercise due diligence in content moderation, data protection, and fraud detection.

As part of a universal cyber law framework, it is essential to hold technology companies accountable for lapses in cybersecurity. Laws must mandate transparency in data handling, swift action against malicious content, and active cooperation with international investigative agencies.

Educating and Empowering the Public

Cyber law is not just about enforcement—it's also about education. There is a dire need to increase **cyber awareness and digital literacy** among users. Many individuals fall victim to cybercrimes simply because they are unaware of basic internet safety practices. Governments, NGOs, and tech firms should invest in training programs, awareness campaigns, and school curricula that promote cyber hygiene and responsible digital citizenship.

Furthermore, universal laws can also empower users by clearly defining their **digital rights and responsibilities**, providing accessible channels for grievance redressal, and ensuring that justice is delivered promptly and fairly.

BIBLIOGRAPHY

ACT & STATUTES

1. California Consumer Privacy Act (CCPA)
2. Computer Fraud and Abuse Act (CFAA)
3. Cyber Security Research and Development Act 2002
4. Digital Personal Data Protection Act (DPDP Act) 2003
5. E-Government Act 2002
6. Federal Information Security Management Act 2002
7. Information Technology Act, 2000

ARTICLES

1. Animesh Sarmah, Roshmi Sarmah, Amlan Jyothi Baruah, A Brief Study of Cyber Crime and Cyber Laws in India, IRJET 1633 (2017)
2. California State Legislature.(2020). California Consumer Privacy Act (CCPA). California Civil Code, Section 1798.100 et seq.
3. Confidential Information Protection and Statistical Efficiency Act Cyber Security Information Sharing Act 2015
4. Cyber Security Research and Development Act 2002 Govinfo, https://www.govinfo.gov/app/details/COMPS-1842 (last visited on Feb 14 2024)
5. European Commission.(2019). EU Cybersecurity Act (Regulation (EU) 2019/881). Official Journal of the European Union.
6. Europol, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited on 26 Feb 2024)
7. IASbaba, https://iasbaba.com/2022/12/national-cybersecurity-strategy/ (last visited on 14 Feb 2024)
8. Indian Computer Emergency Response Team (CERT-In).(2023). Annual Cybersecurity Threat Report.
9. Kuner, Christopher.(2020). The General Data Protection Regulation: A Commentary. Oxford University Press.
10. Lindsay, Jonathan R., & Reiger, David A.(2022). “The Evolution of Cybercrime and Its Legal Responses: A Comparative Perspective.” Journal of Cybersecurity Law, 10(3), 45-78.

11. Ministry of Electronics and Information Technology (MeitY), Government of India.(2023). Digital Personal Data Protection Act, 2023.

12. Onlinewilder, https://onlinewilder.vcu.edu/blog/what-is-homeland-security/ (last visited on 14 Feb 2024)

13. Prabhash Dalei and Tannya Brahme, Cyber Crime and Cyber Law in India: An Analysis, IJHAS Vol.2 No.4, 106 (2013)

14. Solove, Daniel J., & Schwartz, Paul M.(2021). Information Privacy Law. 7th Edition. Aspen Publishers.

15. Techtarget, https://www.techtarget.com/whatis/definition/Cybersecurity-Information- Sharing-ActCISA (last visited on 14 Feb 2024)

16. United States Congress.(1986). Computer Fraud and Abuse Act (CFAA). Public Law No: 99-474.

17. Vaghela, B. P., & Shah, J.(2023). "Cybercrime and Legal Framework in India: A New Paradigm." Indian Journal of Cyber Law, 6(1), 32-50.

18. World Economic Forum (WEF).(2022). Global Risks Report: The Rise of Cybercrime and Fraud.

19. Yoshita Gandhi, "Cyber laws: Comparative study of Indian law & Foreign laws," Journal of Applicable law & Jurisprudence

REPORT

1. Indian Computer Emergency Response Team (CERT-In).(2023). Annual Cybersecurity Threat Report.

2. World Economic Forum (WEF).(2022). Global Risks Report: The Rise of Cybercrime and Fraud.

3. Wilson, J. R. (2007). Terrorist Capabilities for Cyberattack: Overview and Policy Issues. CRS Report for Congress