An Analysis of Cybercrimes Laws in India in comparison with the United States of America and the European Union

*Prof. Gayathri N.M, *Faculty, CMR University, School of Legal Studies*

** Keisiya Glory Babu, *Student, LL.M (Commercial Law), CMR University, School of Legal Studies*

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 analyse 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.

Keywords: Cybercrime, Cyber-Security, Cyberspace, Legal Framework

Introduction

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 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 net[1]. Therefore, it stands to reason that "cyber-crimes" are offenses relating to computers, information technology, the internet, and virtual reality[2]. 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.[3] Cyber warfare is basically a cybercrime that between one nation state and international cross borders.[4] 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."*[5]

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.[6] 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. 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

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

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.[7] The websites may contain malware (such as ransomware) which can sabotage systems and organizations[8]. Or they might be designed to trick users into revealing sensitive information (such as passwords), or transferring money.[9] 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. Email Spoofing is basically a threat that involves sending email messages with a fake sender address.[10] 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[11]. 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.[12] 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. webjacking 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. Cybercrime against society includes cyber terrorism and cyber espionage. 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.[13] Some of the examples are targeting and attacking financial institution to

[7] National Cyber Security Centre, https://www.ncsc.gov.uk/guidance/phishing#:~:text=Business%20Guide%20beforehand.-,What%20is%20phishing%3F,can%20sabotage%20systems%20and%20organisations. (last visited on 14 Feb 2024)
[8] *Id.*
[9] *Id.*
[10] Fortinet, https://www.fortinet.com/resources/cyberglossary/email-spoofing (last visited on 14 Feb 2024)
[11] Fortinet, https://www.fortinet.com/resources/cyberglossary/spyware#:~:text=Spyware%20is%20malicious%20software%20that,device%20without%20the%20user's%20consent. (last visited on 14 Feb 2024)
[12] *Id.*
[13] Wigan Council, https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyber-terrorism.aspx#:~:text=What%20is%20cyber%20terrorism%3F,disruption%20of%20the%20information%20system. (last visited on 14 Feb 2024)

transfer money and cause terror, virus on vulnerable networks, any kind of terror threats using internet.[14] 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.[15]

The Laws of Cybercrime in India

In India, cybercrime laws are primarily governed by the Information Technology Act 2000 and its further amendments. The Act defines various cybercrimes and prescribes punishment for the same. It outlines procedures for investigation and adjudication of cybercrimes. The Information Technology Act, 2000 (hereinafter referred as IT Act, 2000) is the major legislation that governing and regulating cybercrimes in India. This Act was proposed by the parliament of India on 17th October 2000. The Act is based on the United Nations model law on Electronic Commerce (UNCITRAL Model) suggested united nation General Assembly[16]. India is the 12th nation to adopt cybercrimes law based on this model. After the Act was introduced in India, there was an amendment made in some of the legislation in India such as IPC, Indian Evidence Act and included the ambit of cybercrime as an offence. The IT Act, 2000 is having two schedules. Some of the major provisions of the Act are: Section 65 (Tampering with computer source documents)[17] Section 66(Hacking with computer system)[18], Section 66D(Punishment of cheating by personation by using computer resource),[19] Section 66E (Punishment for violation of privacy[20]), Section 66(Punishment for Cyber Terrorism)[21], Section 67 (Publishing of information which is obscene in electronic form[22]), Section 69 (Power to issue directions for inception or monitor [23]), Section 43A(Compensation for failure to protect data[24]). In addition to that nations cyber security policy 2013 vision is to build a secure and resilient cyberspace for citizens, business and government.[25] The 2013 policy provides a roadmap of comprehensive

[14] *Id.*
[15] CrowdStrike, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/ (last visited on 14 Feb 2024)
[16] Geeksforgeeks, https://www.geeksforgeeks.org/information-technology-act-2000-india/ (last visited on 14 Feb 2024)
[17] Information Technology Act 2000 Sec 65
[18] *Id.* sec 66
[19] *Id.* sec 66D
[20] *Id.* sec 66E
[21] *Id.* sec 66F
[22] *Id.* sec 67
[23] *Id.* sec 69
[24] *Id.* sec 43A
[25] National Security Policy 2013

and collective response to deal with cybersecurity within the country[26]. The policy aims at facilitating the creation of a secure computing environment, to enable trust in electronic transactions and to guide stakeholder actions for protection of cyberspace.[27] Furthermore, the National security Council has formulated a draft of national cyber security strategy which addresses the security of national cyberspace[28] which is called National Cyber Security Strategy. It aims to provide a separate legal framework for addressing cyberspace and establishment of an apex body to face threats and to deal complaints.[29] The policy guarantees a reliable, dynamic, safe and robust cyber space for the purpose of financial development in the nation.[30]

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[31]. 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.[32]

[26] What is National Cyber Security Policy 2013 https://www.clearias.com/national-cyber-security-policy-2013/#:~:text=The%20%E2%80%9CNational%20Cyber%20Security%20Policy,security%20in%20the%20digital%20domain. (last visited 14 Feb 2024)
[27] *Id.*
[28] IASbaba, https://iasbaba.com/2022/12/national-cybersecurity-strategy/ (last visited on 14 Feb 2024)
[29] *Id.*
[30] Ekadshi & Deepti Monga, *Comparative analysis of Cyber Security laws of India, United States and United Kingdom*, 9 Int. J. Law 88, 90 (2023)
[31] *Id.*
[32] Indian Evidence Act 1872

The Laws of Cybercrime in United States of America

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.[33] 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.[34] 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.[35] 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.[36] 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 Human Trafficking, Cyber security, Disaster Preparedness, Response and Recovery[37] 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.[38] 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

[33] Jyothi Jain & Rashmi Chaudhary, *Understanding the concept of Cyber Crimes in India vis-à-vis Cyber laws of USA*, 6 IJRAR 427, 429 (2019)
[34] USlegal, https://definitions.uslegal.com/c/counterfeit-access-device-and-computer-fraud-and-abuse-act-of-1984/ (last visited on 14 Feb 2024)
[35] *Id*
[36] Epic,https://epic.org/computer-security-act-of1987/#:~:text=In%201987%2C%20the%20U.S.%20Congress,non%2Dmilitary%20government%20computer%20systems. (last visited on 14 Feb 2024)
[37] Onlinewilder, https://onlinewilder.vcu.edu/blog/what-is-homeland-security/ (last visited on 14 Feb 2024)
[38] Govinfo, https://www.govinfo.gov/app/details/COMPS-1842 (last visited on Feb 14 2024)

FISMA[39] and CIPSEA[40]. 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[41].

The Laws of Cybercrime in European Union

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 cross-border level. The NIS Directive was the first ever EU-wide cybersecurity across the European Union and increase the cooperation between the EU member countries.[42] 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.[43] Moreover, Cybersecurity Act was enforced in 2019, it establishes the European Union Agency for Cybersecurity (ENISA) as a permanent agency[44]. ENISA is tasked with enhancing the overall level of cybersecurity in the EU, providing expert advice, and promoting cooperation between member states.[45] It will be in charge of informing

[39] Federal Information Security Management Act 2000
[40] Confidential Information Protection and Statistical Efficiency Act
[41] Techtarget, https://www.techtarget.com/whatis/definition/Cybersecurity-Information-Sharing-Act-CISA (last visited on 14 Feb 2024)
[42] UpGaurd, https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union (last visited on 24 Feb 2024)
[43] *Id.*
[44] European Commission, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (last visited on 24 Feb 2024)
[45] *Id.*

the public the scheme of certificate and issued certificate through dedicated website.[46] 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.[47] EU Cyber Diplomacy Toolbox was adopted in 2017, it outlines the EU's diplomatic 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.[48]

Comparison of Cyber Crime Laws: India, USA, and EU

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 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. 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

[46] *Id.*
[47] Europol, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited on 26 Feb 2024)
[48] CCDCOE,https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/#footnote_0_4337 (last visited on 25 Feb 2024)

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. 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 (Cert-in) 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 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.

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

Aspect	**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 (Personal Data Protection Bill	Yes (Various sector-specific laws, e.g.,	Yes (General Data Protection

Aspect	India	USA	European Union
	under discussion)	HIPAA)	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

This table provides a broad overview, and it's essential to note that the legal landscape in each jurisdiction may evolve over time. Additionally, the effectiveness of these laws relies on enforcement, international collaboration, and ongoing efforts to address emerging cyber threats.

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 Cyber security 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.

References:

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,"* Journal of Applicable law & Jurisprudence
3. Animesh Sarmah, Roshmi Sarmah, Amlan Jyothi Baruah, *A Brief Study of Cyber Crime and Cyber Laws in India*, IRJET 1633 (2017)
4. Europol, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited on 26 Feb 2024)
5. IASbaba, https://iasbaba.com/2022/12/national-cybersecurity-strategy/ (last visited on 14 Feb 2024)

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

7. Cyber Security Research and Development Act 2002

8. Govinfo, https://www.govinfo.gov/app/details/COMPS-1842 (last visited on Feb 14 2024)

9. E-Government Act 2002

10. Federal Information Security Management Act 2000

11. Confidential Information Protection and Statistical Efficiency Act

12. Cyber Security Information Sharing Act 2015

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

14. European Cybercrime Centre - EC3

15. Europol, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited on 26 Feb 2024)

16. EU Cyber Diplomacy Toolbox

17. CCDCOE, https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/#footnote_0_4337 (last visited on 25 Feb 2024)

18. Ekadshi & Deepti Monga, *Comparative analysis of Cyber Security laws of India, United States and United Kingdom*, 9 Int. J. Law 88, 90 (2023)

19. Indian Evidence Act 1872

20. Jyothi Jain & Rashmi Chaudhary, *Understanding the concept of Cyber Crimes in India vis-à-vis Cyber laws of USA*, 6 IJRAR 427, 429 (2019)

21. Counterfeit Access Device and Computer Fraud and Abuse Act 1984

22. USlegal, https://definitions.uslegal.com/c/counterfeit-access-device-and-computer-fraud-and-abuse-act-of-1984/ (last visited on 14 Feb 2024)

23. Computer Security Act 1987

24. Epic,https://epic.org/computer-security-act-of1987/#:~:text=In%201987%2C%20the%20U.S.%20Congress,non%2Dmilitary%20government%20computer%20systems. (last visited on 14 Feb 2024)

25. Homeland Security Act 2002