CYBERCRIME REGULATION IN INDIA: EFFECTIVENESS OF LAWS, INVESTIGATION PROCEDURE AND JUDICIAL RESPONSE IN COMPARISON WITH THE UNITED STATES

Vishakha Shekhawat[1] & Harika A[2]

ABSTRACT

As the digital landscape evolves, the legal frameworks governing cyber offences have become critical to national security and individual privacy. This paper provides a comparative analysis of cyber law protections in India and the United States, highlighting their distinct legislative approaches and enforcement mechanisms. India primarily relies on the Information Technology (IT) Act, 2000 (as amended in 2008), a centralized framework that combines electronic governance with criminal penalties for offenses like hacking and data theft. In contrast, the United States employs a decentralized framework, utilizing a web of federal laws such as the Computer Fraud and Abuse Act (CFAA) alongside various state-level regulations. The study examines key differences in jurisdictional challenges, definitions of "cybercrime," and the balance between national sovereignty and individual privacy rights. While India focuses on state-centric security and digital commerce, the US framework emphasizes consumer privacy and advanced specialized enforcement. The research shows that both countries have a hard time actually punishing hackers and figuring out which police should handle a crime when it happens online. To get better at stopping global hackers, India needs better digital labs for finding evidence and needs to sign international agreements (like the Budapest Convention) to work more closely with other countries. The present study believe that although India has a centralized legislative system, its effectiveness is limited by not signing the Budapest Convention. While the US uses this international treaty to make cross- border evidence sharing easier, India relies on slower Mutual Legal Assistance Treaties (MLATs), which creates major obstacles in investigating crimes that occur overseas. The present study argues that the shift toward the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, improves the process of collecting digital evidence, yet there is still a gap between India's local "Cyber Cells" and the US's well- coordinated federal-state task forces. The Indian judiciary has demonstrated positive intentions through important rulings, but the backlog of cases continues to be a significant issue. Shreya

[1] Assistant Professor, School of Law, Dayananda Sagar University, Bangalore
[2] LL.B. IV Sem student, School of Law, Dayananda Sagar University, Bangalore

Singhal v. Union of India (2015): This case struck down Section 66A of the IT Act, ensuring that cyber laws do not infringe on free speech. Justice K.S. Puttaswamy v. Union of India (2017): This ruling confirmed privacy as a fundamental right, laying the groundwork for data regulations in India. Van Buren v. United States (2021): A case from the US Supreme Court that limited the reach of the Computer Fraud and Abuse Act (CFAA). It provides a lesson in "judicial narrowing" to prevent the over-criminalization of minor technical violations. The study concluded that for India to achieve the level of enforcement seen in the US, it needs to address its position on the Budapest Convention or create a strong alternative for international cooperation. The focus should shift from simply passing laws to building capacity by equipping the police and judiciary with the technical forensics necessary to tackle AI- driven threats.

Keywords: Cybercrime Regulation, IT Act 2000, Computer Fraud Abuse Act (CFAA), Budapest Convention, Digital Evidence, BNSS 2023, Cross-border Investigation, Judicial Response, Data Sovereignty, and Privacy Rights.

INTRODUCTION:

Cybercrime Regulation in India-

The internet is an essential part of everyday life in the modern world. There are some digital platforms that are widely used for communication, education, commerce, banking and governance. Whereas digitalization has improved efficiency and accessibility, it also increases vulnerability to cybercrimes. Cyber-crimes are committed using mobile devices and networks, which often make detention complex due to cross-border jurisdiction. India has made rapid digital growth under initiatives such as digital India which has made cyber security a major concern. Cyber-crimes cause not only financial loss but also mental distress, reputational harm, and violation of fundamental rights. Hence, an effective and updated legal framework is essential to ensure digital safety and justice.[3] Cyber-crime is an illegal activity carried out using computers, digital devices, or networks, either as a means to commit the offence or as the target itself. These crimes can be directed against individuals, organizations, or even the government.

Types of Cyber Crimes:[4]

- Hacking or accessing systems without permission

[3] Cyber Crimes In India: A Legal Analysis With Special Reference To The Information Technology Act, 2000, BNS, 2023 And BNSS, 2023
[4] ibid.

- Online money fraud
- Stealing someone's identity
- Phishing and email scams
- Cyberstalking and online harassment

India aims to transform into an information-based society through the "Digital India" initiative, where the government, private sector, and individuals rely heavily on the internet for important transactions and storing data in the cloud. This increasing dependence also makes the country more vulnerable to cybercrimes.[5] Globally, many countries are addressing cybercrime by joining the Council of Europe's Budapest Convention on Cybercrime. However, India has been hesitant to become a part of this agreement. This article critically examines the reasons why India should consider signing the Budapest Convention. The article is divided into three parts. The first part explains the Budapest Convention, including its development and the types of crimes it covers. The second part discusses why such a convention is necessary to deal with cybercrime, considering factors like the rapid growth of internet use and challenges of jurisdiction. The third part looks at India's reasons for not signing the convention and also explains why India should reconsider and join it.[6]

Evolution of Cybercrime Regulation in India:

The development of cyber laws in India has closely followed the country's rapid growth in digital technology. In the late 1990s, the internet was still new, and cybercrimes were not very common. Most incidents involved simple acts like basic hacking or defacing websites. However, as technology became more accessible and people started using the internet in their daily lives, these activities slowly turned into more serious problems. With the rise of online banking, shopping websites, and social media in the early 2000s, cybercrimes increased not only in number but also in completely.[7] To deal with these growing issues, the government introduced the Information Technology Act, 2000[8]. This was an important step, as it officially recognized cyber offences and gave legal support to digital transactions. The law covered offences like hacking, identity theft, and cyberstalking. It also helped promote e-governance

[5]https://www.researchgate.net/profile/JuneedIqbal/publication/322245372_Cybercrime_in_India_Trends_and_Challenges/links/5a4e040c458515a6bc6ea9e3/Cybercrime-in-India-Trends-and-Challenges.pdf
[6] Keyser M, "The Council of Europe Convention on Cybercrime," Computer Crime (Routledge 2017)
[7] Chhachhar V and Niharika, "Enforcement of International Law in India-Constitutional and Legal Framework" (2021) 02 International Academic Journal of Law 1
[8] THE INFORMATION TECHNOLOGY ACT, 2000 ACT NO. 21 OF 2000

and online business by allowing the use of digital signatures and electronic contracts.[9] However, the law was not perfect. Technology was developing very quickly, and many types of cybercrimes that we see today were not even thought of when the Act was first made. Because of this, older laws like the Indian Penal Code, 1860 were used to handle online crimes. Sections related to cheating, threats, and defamation were applied to cases such as online fraud, cyberbullying, and harassment. But this method was not always effective, as these laws were not originally designed for digital offences. To improve the situation, the law was amended in 2008. The updated Act included new provisions to deal with serious issues like cyber terrorism, child pornography, data breaches, and violations of privacy. It also introduced stricter punishments for certain offences, showing that the government was taking cybercrime more seriously.[10]

Even with better laws in place, there were still problems with enforcement. Many police officers did not have proper training to handle digital evidence, and several areas lacked specialized cybercrime units or modern technology. Because of this, many victims chose not to report crimes like online blackmail or harassment, either because they did not trust the system or felt embarrassed. Over time, things have started to improve. Law enforcement agencies are now receiving training in cyber forensics, and more cybercrime cells are being set up across the country. Public awareness has also increased, helping people understand online risks and protect themselves better. India is also working with other countries to deal with cybercrimes that go beyond national borders. Overall, India's journey in dealing with cybercrime shows a continuous effort to keep up with changing technology. As cyber threats become more advanced, the legal system will also need to keep adapting to effectively handle new challenges.

Key Legislations and Regulations:

1. **Information Technology Act, 2000:** This is the main law in India that deals with digital transactions and cybercrimes. It gives legal recognition to electronic records and digital signatures, supports online business, and provides punishment for cyber offences.[11]

[9] Ibid 2 para.
[10] "EU Institutional Enforcement of EU Environmental Law: The General Legal Framework," , Enforcement of European Union Environmental Law (Routledge 2015) <https://doi.org/10.4324/9780203074848-10> accessed April 14, 2026
[11] The Information Technology (Amendment) Act, 2008, Acts of Parliament, 2008 (India).

2. **Information Technology (Amendment) Act, (2008):** This amendment improved the original law by introducing stricter rules for cybercrimes. It increased penalties and added provisions to protect important information systems from new and emerging cyber threats.[12]
3. **Personal Data Protection Bill:** This bill focuses on protecting people's privacy. It sets rules on how personal data should be collected, used, stored, and shared. It also places responsibilities on organizations handling such data and includes provisions like data localization.
4. **National Cyber Security Policy:** Outlines India's plan to boost cybersecurity through proactive steps, skill development, and teamwork with stakeholders to make cyberspace more secure.[13]

The Need for cybercrime Regulation in India[14]

In today's digital world, cyber law has become very important. It acts as a legal system that controls activities on the internet and digital platforms. Its main aim is to regulate online spaces, protect individuals, businesses and the government from cyber threats, and ensure safety, privacy, and responsible use of technology.

There are several reasons why cyber laws are necessary:

Cyber laws play a crucial role in protecting individuals and society in the digital age. They provide legal remedies and penalties to prevent and punish cybercrimes such as hacking, identity theft, phishing, and cyberstalking. These laws also ensure the security of digital transactions and e-commerce by safeguarding online payments, regulating electronic contracts, and protecting consumer rights. In addition, cyber laws focus on data protection and privacy by regulating how personal information is collected, used, and stored, as seen in frameworks like the GDPR in Europe and the Personal Data Protection Bill in India. They also help protect intellectual property rights by securing digital intent such as copyrights, patents, and trademarks from misuse. Furthermore, cyber laws play an important role in preventing cyber terrorism and addressing threats to national security by enabling governments to monitor and take action against harmful activities. Lastly, they regulate social media platforms by

[12] INDIAN JOURNAL OF LEGAL REVIEW.
[13] Supra note 362
[14] Ph.D. VS, Browsing the Cyber Laws of India: A User's Guide (Vikas Sharma PhD 2023)

addressing issues like fake news, hate speech and misinformation, thereby promoting a safer and more responsible online environment.

Global Cyber Law Frameworks

Some important cyber law frameworks around the world include the Information Technology Act, 2000[15] in India, which deals with cybercrimes, data protection, and regulations related to online transactions. In the European Union, the General Data Protection Regulation (GDPR) focuses on protecting personal data and ensuring user privacy. In the United States, the "Computer Fraud and Abuse Act"[16] addresses offences such as hacking and unauthorized access to computer systems. Additionally, the Budapest Convention on Cybercrime is an international agreement aimed at promoting cooperation among countries to combat cybercrime effectively.

Investigation Procedure in India:

Investigation of cybercrime requires specific technical expertise and scientific equipment; without these, the probe cannot begin. India's legal system has set up various processes, rules, and regulations that are codified in statutes. Technological advances have helped development, yet they have also made digital India a fast-growing environment for crimes. Cybercrimes typically cross geographical boundaries, and cyber criminals exploit the internet's speed and anonymity to carry out various criminal activities. These crimes can cause severe damage and create genuine threats for victims all over the world, not only for cyber- crime victims. To manage cyber-crimes, the Criminal Investigation Department (CID) in various cities established the Cyber Crime Cells in different parts of India, and the IT Act of 2000[17] clarified this legal framework.

Cybercrime investigation involves examining and collecting important digital evidence from networks such as the internet or local systems to identify the offender and understand their intentions. It requires investigators to have knowledge of computers, including software, operating systems, file systems, networks and hardware. They must understand how these elements work together so they can determine what happened, why happened, when it occurred, who was responsible, and how such incidents can be prevented in the future. Under Section 78 of the Information Technology Act, only a police officer of at least the rank of

[15] Information Technology Act 2000.
[16] Computer Fraud and Abuse Act 1986 (US).
[17] The Information Technology Act, 2000.

Inspector is authorized to investigate offences under the Act. Further, Section 80 empowers such officers, or other authorized officials, to search, seize, investigate, and arrest individuals suspected of committing cyber offences.[18]

CYBERCRIME INVESTIGATION METHODS

The methods used in cybercrime investigations vary depending on the nature of the offence and the agency handling the case. However, most cybercrimes are generally examined using a set of common investigation techniques that help authorities identify, analyze, and solve digital offences.[19]

COMPLAINT

The person who becomes a victim of cybercrime can approach a cybercrime cell to file a complaint, either through online platforms or by visiting the office in person. If the complaint is not made to a cybercrime cell, the victim also has the option to register an FIR at a local police station under Section 154 of the Criminal Procedure Code. In situations where the police refuse to accept the complaint, the victim can seek help by approaching the Judicial Magistrate of the concerned district.

COLLECTING INFORMATION

Once the complaint is received, the investigation process begins with gathering relevant details about the incident. The investigator collects information from the victim, witnesses, and other available sources. This step focuses on identifying key facts, possible evidence and suspected individuals, as well as understanding how the offence was planned and carried out.

TRACKING

After gathering basic information, investigators move to the tracking stage. In this phase, they work closely with internet service providers and network-related organizations to trace digital activities linked to the offence. This includes collecting records such as connection logs, browsing history, and other technical details related to the attack. This process can take time because access to such data usually requires proper legal authorization or a court order.

FORENSICS

After collecting the necessary information and evidence, the investigator forwards it to the

[18] The section 78 provided under the Information Technology Act, 2000.
[19] https://ijrpr.com/uploads/V4ISSUE4/IJRPR12115.pdf

forensic department for detailed examination. The forensic experts analyze various digital elements such as network activity, raw data, hard drives, file systems, cache memory, and RAM. During this stage, they carefully examine systems files, service logs, emails, and browsing history to trace any clues related to the offence. Based on these findings, investigators continue to follow digital trails to understand how the crime was committed.[20]

IDENTIFYING THE OFFENDER

Once the forensic analysis is completed, a report is prepared and shared with the investigating officer. Using this report, the investigator identifies the person responsible for the cybercrime. After confirming the suspect's involvement, appropriate legal action is taken in accordance with the provisions of the Criminal Procedure Code (Cr.P.C).

NATIONAL CYBER SECURITY COORDINATION CENTRE (NCSC)

The NCSC is a government body responsible for coordinating efforts among various national agencies to handle and prevent cyber-related threats. It plays an important role in maintaining cybersecurity at the national level.

CYBERCRIME CELL

Cybercrime cells are specialized units that deal with the investigation of cyber offences. These units have been established in major cities across India. However, there is still a need to strengthen these cells by improving technical infrastructure and ensuring the availability of trained and skilled professionals.

CBI's SPECIAL UNITS

To fight cybercrime effectively, the Central Bureau of Investigation (CBI) has set up special units for different purposes. These include a research unit that studies cybercrime and finds better ways to deal with it, an investigation cell that handles cybercrime cases, a forensic lab that examines digital evidence, and a monitoring center that keeps track of network activities to identify and prevent cyber threats.[21]

EXTENDED MODEL OF CYBERCRIME INVESTIGATIONS

The process of cybercrime investigation generally follows a systematic and organized approach. It begins with awareness, where it is identified that a cyber incident has taken place

[20] Supra p. 4701
[21] https://www.asianlaws.org/blog/adjudicating-officers-for-cyber-crimes-appointed-in-india/

and requires proper investigation. This is followed by authorization, where the investigating authorities obtain the necessary legal permissions, such as warrants, to proceed with the inquiry. Once permission is granted, the next step is planning, where investigators develop a strategy based on the information available. After this, notification takes place, in which relevant parties are informed that an investigation is being conducted. The investigators then move to the stage of search and identification, where they locate potential sources of digital evidence related to the offence. Following this, collection of evidence is carried out by securing and gathering all relevant materials. The collected evidence is then carefully transported to a suitable location for further examination and is properly stored to prevent any damage or contamination. The next stage is examination, where the evidence is analyzed using specialized tools and techniques.

Based on this analysis, investigators form a hypothesis, which is a possible explanation of how the cyber incident occurred. This hypothesis is then presented before a court or the concerned authority. Finally, the process includes proof or defense, where the findings are either supported or challenged with evidence. The last stage is dissemination, where the knowledge and insights gained from the investigation are shared to help improve future cybercrime investigations and prevention strategies.

ADJUDICATION OF CYBERCRIMES

The system for handling cyber offences in India is mainly governed by the Information Technology Act, 2000[22]. This law provides a structured mechanism to deal with both civil and criminal cyber issues through adjudicating officers, who act like quasi-judicial authorities. These officers have the power to decide cases, impose fines, and award compensation to victims. If a person is not satisfied with the decision, they can file an appeal before the Cyber Appellate Tribunal, which is headed by a chairperson and members appointed by the Central Government. Further, a second appeal can be made to the High Court within 60 days of the Tribunal's decision.[23]

ADJUDICATING OFFICER

Under the Act, the Central Government appoints adjudicating officers to handle cases related

[22] Information Technology Act 2000.
[23] Rai D, "Dispute Resolution Mechanism of Cyber Laws in India" (iPleaders, December 27, 2021) <https://blog.ipleaders.in/dispute-resolution-mechanism-of-cyber-laws-in-india/?amp=1> accessed April 14, 2026

to cyber law violations. These officers are responsible for deciding penalties when the provisions of the Act are violated. If any party is not satisfied with their decision, they can appeal before the Cyber Appellate Tribunal, which reviews such cases.

COMPENSATION THROUGH ADJUDICATION:

Section 43 of the IT Act provides that a person who causes damage to a computer system or network can be held liable to pay compensation, which may go up to one crore rupees. Such liability arises in cases like unauthorized access to a computer, copying or downloading data without permission, introducing harmful software like viruses, damaging systems, blocking access, committing fraud using computers, or helping others gain illegal access.[24]

Effectiveness of Law in India dealing with cybercrime:

Cyber laws in India are mainly based on the Information Technology Act, 2000. [25]When this law was first introduced, the internet was still developing in the country. Its main aim was to give legal recognition to electronic records and digital signatures, making online transactions safer and more reliable. Over time, the law was expanded to include provisions for various cyber offences and to give authorities the power to investigate and take action against such crimes. The IT Act was India's first major step in regulating activities in cyberspace. Initially, it focused on making electronic documents and contracts legally valid. However, as misuse of technology increased, the law was updated to address cybercrimes. It now covers offences such as hacking, identity theft, and online obscenity, which are defined under different sections of the Act. While these provisions are important, their implementation is not always consistent.

In 2008, significant amendments were made to strengthen the law. New provisions were added to deal with serious threats like cyber terrorism, and stricter rules were introduced for data protection. Certain sections also allow the government to monitor and intercept digital information for security reasons, although this has raised concerns about misuse and lack of proper safeguards. Additionally, companies that are required to protect sensitive personal data may be held responsible if they fail to do so. Despite these developments, the law is often seen as reactive rather than proactive, as it tends to respond to technological changes instead of

[24] Asian School of Cyber Laws, "Asian School of Cyber Laws" (Tech Law Blog, November 11, 2002) <https://www.asianlaws.org/blog/adjudicating-officers-for-cyber-crimes-appointed-in-india/> accessed April 14, 2026

[25] Information Technology Act 2000

anticipating them. As technology continues to evolve rapidly, there is a constant need to update and improve cyber laws to effectively deal with new challenges.

Other Relevant Legislations

Indian Penal Code, 1860: Besides the IT Act, various other statutes help regulate online activities and enforce digital accountability. The Indian Penal Code of 1860, although noy originally crafted for cyber offences, has been applied in many online fraud cases, especially under Sections 419 and 420, which address cheating and impersonation. These provisions are commonly used together with IT Act clauses to prosecute cybercriminals effectively.[26]

Companies Act, 2013: The Companies Act of 2013 also includes obligations regarding data and cybersecurity for corporate bodies. It requires directors and senior management to implement suitable measures to safeguard data and maintain secure information systems. Failure to comply can result in corporate bodies. It requires directors and senior management to implement suitable measures to safeguard data and maintain secure information systems. Failure to comply can result in corporate liability and criminal consequences, particularly in cases of financial misconduct or breaches.[27]

Data Protection Bill: Another vital legislative piece, yet to be enacted, is the Data Protection Bill, expected to become India's primary law governing personal data and protection. Inspired by global standards like the European Union's General Data Protection Regulation (GDPR), the Bill seeks to establish a comprehensive framework for data collection, processing, and consent management, while setting up a Data Protection Authority. Its eventual enactment is anticipated to greatly enhance legal safeguards for internet users and imposes stricter duties on data handlers.

Overall cyber legal framework: Collectively, these laws from the foundation of India's cyber legal structure. However, the fragmented and sometimes outdated nature of these statutes underscores the urgent need for a unified, modern, and coherent legal regime to address the complex realities of cyberspace.

The recent amendments and acts dealing with cyber law in India (2023-2026):

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026: This amendment notified on February 10, 2026, focuses on

[26] The Indian Penal Code, 1860
[27]THE COMPANIES ACT, 2013

"Synthetically Generated Information" (SGI) such as deepfakes. It mandates that platforms remove unlawful SGI within 3 hours and highly sensitive content (like non-consensual deepfake nudity) Intermediaries must also implement mandatory labeling and embed metadata for AI- generated content.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Second Amendment Rules, 2026: Notified on March 30, 2026, these rules extend government oversight to user-generated news and current affairs content. They grant the Ministry the power to issue binding ministerial directions and require intermediaries to follow a "Code of Ethics" to maintain their legal immunity under Section 79 of the IT Act.

Digital Personal Data Protection (DPDP) Rules, 2025: Notified on November 14,2025, these rules fully operationalize the DPDP Act of 2023. They establish a "SARAL" (Simple, Accessible, Rational, and Actionable) framework for data privacy, including clear consent notices, the registration of India-based "Consent Managers," and the setup of a digital-first Data Protection Board.

Jan Vishwas (Amendment of Provisions) Act, 2026: This act decriminalizes 717 provisions across 79 Central Acts to improve the "Ease of Doing Business". In the context of cyber law, it replaces imprisonment with monetary penalties for minor procedural lapses under the IT Act, such as Section 67C regarding data retention by intermediaries.

Telecommunications Act, 2023: Enforced in a staggered manner throughout 2024, this act replaces colonial-era laws with a modern framework for digital connectivity. Section 22 empowers the government to declare "Critical Telecommunication Infrastructure" (CTI) and set cybersecurity standards for networks. It also introduced "SIM binding" for messaging apps to prevent digital impersonation and fraud.

New Criminal Laws (BNS, BNSS, BSA), 2024: Implemented on July 1, 2024, these laws (Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Adhiniyam) replaced the IPC, CrPC, and Indian Evidence Act. The BNS explicitly defines "organized cybercrime" (Section 111) and "cyber-stalking" (Section 78), while the BSA grants electronic records the same legal status as paper documents.[28]

Promotion and Regulation of Online Gaming Act, 2025: Assigned to on August 22, 2025, this act prohibits all forms of "online money games" (games involving financial stakes). It

[28] The Bharatiya Sakshya Adhiniyam, 2023 (ACT NO. 47 OF 2023) [As on the 6th October, 2026]

establishes a National Online Gaming Commission (NOGC) to regulate e-sports and social games while imposing strict penalties, including up to three years of imprisonment for offering prohibited money games.

CERT-In Cybersecurity Guidelines, 2025 (CISG-2025-02): effective July 25, 2025, these guidelines mandate annual third-party cybersecurity audits for all enterprises. They also expand the "Bill of Materials" (BOM) requirements to include software (SBOM), hardware (HBOM), and AI (AIBOM) components to serve as first-line incident response tools.

JUDICIARY RESPONSE

Cybercrimes happen in the online world and pose big challenges for law enforcement because they are hard to track down. Unlike regular crimes, there is no physical presence or tangible clues like fingerprints, making it tough to investigate. Traditional methods of gathering evidence often don't work well for cybercrimes, showing the need for new legal approaches.[29] The Supreme Court of India, in the case of State of Punjab v. Amritsar Beverages Ltd, pointed out the difficulties involved in dealing with cybercrimes and the gaps that still exist in the current legal framework. The Court observed that although the Information Technology Act covers several types of cyber offences, it does not fully address all the challenges, especially those that require advanced technical or scientific expertise.

A major issue in pursuing cybercrime is figuring out which jurisdiction applies, as cyberspace crosses borders. Accused often challenge jurisdiction, exploiting the global nature of the internet, making prosecution complicated, especially when accused and victims are in different countries. The Shreya Singhal case[30] shows the judiciary's evolving approach to balancing free speech with regulating harmful online activities. The Supreme Court struck down Section 66A of the IT Act, ruling it violated Article 19 (1)(a) of the Constitution[31], highlighting cyberspace as a platform for free expression with constitutional protections. Cybercrimes create unique legal challenges because they are not physical in nature and often take place across different countries. Issues like deciding jurisdiction, collecting reliable digital evidence, and coordinating with foreign authorities make prosecution more complicated. Although Indian courts have taken important steps in interpreting cyber laws, there is still a need for reforms to address both procedural and legal gaps, especially in maintaining a balance between freedom

[29] https://ijrar.org/papers/IJRAR24D1029.pdf
[30] Shreya Singhal Vs. Union of India, AIR 2015 SC 1523
[31] Constitution of India 1950, art 19(1)(a).

of speech and necessary regulation.

The Sanjay Kumar case illustrates financial crimes via technology, where the accused manipulated bank software for fraud. The judgement underscores the need for heightened scrutiny of technology-enabled financial crimes. Cases like Cubby, Inc. v. CompuServe, Inc. address ISP liability for third party content, establishing the "Control over Content" principle – ISPs are not liable without editorial control or knowledge of defamatory content.[32] Indian judiciary decisions reflect a progressive approach balancing individual rights and accountability in cyberspace, emphasizing constitutional protections like freedom of speech. However, gaps remain, urging reforms for a comprehensive legal system handling cyberspace's dynamic nature.

Before the enactment of the Information Technology Act, 2000 and its 2008 amendment, the approach of Indian courts towards obscenity and pornography was mainly based on traditional legal provisions, especially Section 292 of the Indian Penal Code, 1860. Courts generally focused on protecting public morality and decency while deciding such cases. In the case of Sukanto Haldarv. State of West Bengal[33]The court found the accused guilty for publishing an obscene magazine titled "Nara Nari" and imposed punishment under Section 292, showing the strict stance taken against obscene publications during that time.[34] Another important case is Ranjit D. Udeshi v. State of Maharashtra[35], where the Supreme Court held the book Lady Chatterley's Lover to be obscene. The Court also tried to distinguish between obscenity and pornography and emphasized that any material which negatively affects public morality and decency can be restricted. Overall, before the introduction of specific cyber laws, the judiciary mainly relied on moral standards and existing criminal laws to deal with obscenity and pornography, focusing on their potential impact on society.

Cybercrime Regulation in the United States (Not Present in India):

Cybercrime regulation in the United States is quite different from India, as it is based on a combination of federal and state laws rather than a single comprehensive law. At the federal level, laws like the Federal Information Security Modernization Act (FISMA), introduced in 2002, require government agencies to protect and secure their data. Another important law is the Cybersecurity Information Sharing Act (CISA) of 2015, which allows private companies

[32] In Cubby, Inc v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y.1991)
[33] Sukanto Haldar v State of West Bengal AIR 1952 Cal 214.
[34] Bombay H.C., Writ Petition No.1611 of 2001,28th September. 8 C.C.N.O. 3700686/PS/2009.
[35] Ranjit D Udeshi v State of Maharashtra AIR 1965 SC 881.

and government bodies to share information about cyber threats with the Department of Homeland Security.[36] In addition to federal laws, individual states in the U.S. also have their own cybersecurity and privacy regulations. For example, the California Consumer Privacy Act (CCPA),[37] which came into force in 2020, gives individuals greater control over their personal data. It allows people to know what data is collected, request its deletion, and opt for the sale of their personal information. Similarly, in New York, the Department of Financial Services enforces strict cybersecurity rules for financial institutions.[38]

The U.S. also has several agencies responsible for handling cyber threats and ensuring cybersecurity. These include the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA). These agencies work together to prevent, detect, and respond to cybercrimes. Additionally, the Government Accountability Office (GAO) monitors whether federal agencies are properly following cybersecurity laws and policies.[39] For reporting cybercrimes, the United States provides multiple options. Individuals can contact the United States Computer Emergency Readiness Team (US-CERT) or file complaints through platforms such as the Federal Trade Commission (FTC) and the Internet Crime Complaint Center (IC3), which specifically handles online fraud and cyber offences. Overall, the U.S. follows a sector-specific and decentralized approach to cyber regulation. Instead of having one single law like India's Information Technology Act, the U.S. relies on multiple laws that address different aspects of Cybersecurity. Key examples include the Children's Online Privacy Act (ECPA)[40] which safeguards electronic communications, and the Computer Fraud and Abuse Act (CFAA), which deals with hacking and unauthorized access. This system allows individual states to create laws suited to their needs, making the framework flexible. However, it can also lead to differences in rules and challenges in maintaining uniform enforcement across the country.

Privacy and Data Protection

India and the United States follow different approaches when it comes to data protection. In India, the Digital Personal Data Protection Act, 2023 focuses mainly on obtaining a person's consent before collecting or using their personal data. The law gives individuals more control over their information and places responsibilities on organizations, known as Data Fiduciaries,

[36] https://www.ijnrd.org/papers/IJNRD2403210.pdf
[37] California Consumer Privacy Act 2018 (US).
[38] Id note 26
[39] https://www.scriptonet.com/journal/comparison-of-cyber-laws-india-vs-usa/
[40] Children's Online Privacy Protection Act 1998 (US)

that handle such data. It also provides for penalties if these rules are not followed. This Act is an important step towards strengthening data protection in India. However, one major concern is the absence of a strong and fully independent regulatory authority, unlike the system followed in Europe under GDPR. Because of this, there are doubts about how effectively the law will be enforced and whether it will provide sufficient protection in practice. While the Act shows progress, its real impact will depend on how well it is implemented.

In contrast, the United States does not have a single comprehensive law for data protection. Instead, it follows a fragmented system with multiple laws at both federal and state levels, each dealing with specific sectors. For example, the California Consumer Privacy Act (CCPA) is a well-known state law that gives individuals rights over their personal data, such as knowing what information is collected, requesting its deletion, and opting out of its sale. Apart from state laws, the U.S. also has federal laws that apply to particular industries. One example is the Health Insurance Portability and Accountability Act (HIPAA), which deals with the protection of medical information. This sector-based approach allows laws to address specific privacy concerns, but it can also lead to differences and lack of uniformity across the country.

Cybercrime and Enforcement

In India, cybercrime is mainly dealt with through two important laws-the Information Technology Act, 2000 and the Indian Penal Code. The Act specifically focuses on offences committed in the digital space, while the IPC is a general criminal law that can also be applied to cyber offences when required. Along with these laws, agencies such as Cyber Crime Cells and the Indian Computer Emergency Response Team (CERT-In) play a key role in monitoring and responding to cyber threats. CERT-In acts as the central agency for handling cybersecurity incidents, while Cyber Crime Cells at both state and national levels investigate individual cases. Despite these measures, dealing with cybercrime in India remains challenging. Factors such as lengthy procedures, lack of specialized training among police officers, and a heavy workload often slow down investigations and court proceedings. These issues make it difficult to effectively control and prevent cyber offences.

In comparison, the United States has a more advanced and well-equipped system for tracking cybercrime. Several federal agencies are involved in investigating and prosecuting such offences, including the Federal Bureau of Investigation (FBI), the Cybersecurity and

Infrastructure Security Agency (CISA)[41], and the Secret Service. The FBI usually handles major and complex cybercrime cases while CISA focuses on strengthening cybersecurity and responding to incidents. The Secret Service mainly deals with cybercrimes related to financial fraud, using its expertise in financial investigations. The U.S. system benefits from coordination among multiple agencies, clear legal frameworks, and significant investment in technology, which improves its ability to detect and control cybercrime. It also cooperates with other countries, making it easier to handle cross-border cyber offences and share important information. However, despite these advantages, cybercrime continues to evolve rapidly, and law enforcement agencies in the U.S. still face ongoing challenges in keeping up with new and sophisticated threats.

HYPOTHESIS

The research is based on the hypothesis that cybercrime regulation in India, mainly governed by the Information Technology Act, 2000, is not fully effective in practice due to issues such as lack of proper enforcement, limited technical expertise among investigation authorities, and delays in the judicial process.

In comparison, the United States has a more efficient cybercrime control system because of advanced investigative mechanisms, specialized agencies, and stronger implementation of laws like the Computer Fraud and Abuse Act. However, it is also assumed that India does not lack legal provisions, but rather faces challenges in implementation and infrastructure.

SUGGESTIONS

To improve the effectiveness of cybercrime regulation in India, several measures can be adopted. Firstly, there is a need to strengthen investigation by establishing specialized cybercrime units in every district and providing proper technical training to police officials in areas like digital forensics and artificial intelligence Secondly, the judicial system should be made more efficient by setting up special cybercrime courts to ensure speedy trials and reduce delays. Public awareness is also essential, and citizens should be educated about online frauds, phishing, and data protection. Further, legal reforms are necessary to update outdated provisions of the IT Act and introduce stricter punishments for serious offences. India can also adopt certain best practices from countries like the United States and improve international cooperation to tackle cross-border cybercrimes effectively.

[41] Cybersecurity Information Sharing Act 2015 (US).

In addition to existing measures, some innovative solutions can be introduced to address cybercrime more effectively. One such idea is the creation of a "cybercrime rating system" where websites and applications are rated based on their security standards, which can be supported by provisions like Section 43 and Section 66 of the Information Technology Act, 2000 that deal with unauthorized access and hacking. Another suggestion is to establish a "digital police station" for easy online complaint filing, aligning with the need for speedy justice recognized in cases like Maneka Gandhi v. Union of India, where the Supreme Court emphasized fair and reasonable procedure under Article 21. Introducing cybercrime insurance can help victims recover financial losses, especially in fraud-related offences under Section 66D of the IT Act. Further, an AI-based early warning system can be developed to detect suspicious activities and protect users' right to privacy, as recognized in K.S. Puttaswamy v. Union of India. A national network of cyber volunteers, including ethical hackers, can assist authorities, while maintaining accountability under Section 72 of the IT Act relating to breach of confidentiality.

Lastly, making can be justified in light of corporate responsibility highlighted in cases like Shreya Singhal v. Union of India, where the Court stressed the need for balanced regulation of the internet. These suggestions can significantly strengthen cybercrime regulation in India.

Conclusion:

Cybercrime is growing rapidly in India, although laws like the Information Technology Act, 2000 provide a strong legal framework, their effectiveness is still limited due to problems in implementation, lack of technical skills, and delays in investigation and judicial process. When compared to the United States, which has advanced laws like the Computer Fraud and Abuse Act and better enforcement mechanisms, India still has scope for improvement. However, India has the potential to strengthen its cybercrime system by improving investigation techniques, creating awareness among people, and adopting new technologies like artificial intelligence. The introduction of innovative ideas such as digital police stations, cybercrime insurance, and security rating systems can further help in preventing cyber offences. Overall, with proper implementation of laws, better infrastructure, and learning from global practices, India can effectively control cybercrime and ensure a safer digital environment for its citizens. Therefore, India should focus not only on strengthening its domestic legal system but also on increasing international cooperation, adopting global standards, and using advanced technologies. By improving enforcement, encouraging innovation, and possibly moving towards frameworks

like the Budapest Convention, India can build a more effective cybercrime regulation system and ensure better protection for its citizens in the digital world.