International Journal of Management and Humanities (IJMH)
ISSN: 2394-0913 (Online), Volume-12 Issue-2, October 2025

Cybersecurity Laws in India and Beyond: A Comparative Legal Perspective

Madhuri Paradesi, P. Jogi Naidu, Goriparthi. Naresh

Abstract: ***In an increasingly Digitalized world, cybersecurity has emerged as a crucial pillar of national security, economic stability, and individual privacy. With the rise in cyber threats, including data breaches, ransomware attacks, and state-sponsored cyber warfare, governments worldwide have enacted comprehensive cybersecurity laws to safeguard essential systems, businesses, and individuals. The comparative analysis of cybersecurity laws in India and other major jurisdictions, such as the United States, the European Union, and China, to assess their effectiveness, enforcement mechanisms, and adaptability to emerging threats. India's cybersecurity legal framework is primarily governed by "The Information Technology Act, 2000, alongside the recently implemented "Digital Personal Data Protection Act, 2023". It examines the scope and limitations of these laws, particularly in addressing modern cyber risks and ensuring compliance with global standards. Comparatively, the paper delves into the cybersecurity policies of the United States, including the Cybersecurity Information Sharing Act and Executive Orders on critical infrastructure protection; "The European Union's GDPR" and the "Network and Information Systems" (NIS) Directive; and also mandates strict government control over cyber operations and data governance. The study concludes with recommendations for strengthening India's cybersecurity legal framework by integrating global best practices, enhancing enforcement capabilities, and fostering international collaboration.***

Keywords: Cybersecurity, The Information Technology Act, 2000, The Digital Personal Data Protection Act, 2023, National Security, Public-Private Partnerships.

Nomenclature:
NIST: National Institute of Standards and Technology
GDPR: General Data Protection Regulation
CFAA: Computer Fraud and Abuse Act
COPA: Child Online Protection Act
HIPAA: Health Insurance Portability and Accountability Act
FISMA: Federal Information Security Modernisation Act
DHS: Department of Homeland Security
FBI: Federal Bureau of Investigation
CERT: Computer Emergency Response Team
NIS: Network and Information System
CISA: Cyber Security Information Sharing Act
UK-GDPR: United Kingdom Data Protection Regulation
HSA: Homeland Security Act
ITAA: Information Technology Act

Manuscript received on 21 September 2025 | First Revised Manuscript received on 28 September 2025 | Second Revised Manuscript received on 09 October 2025 | Manuscript Accepted on 15 October 2025 | Manuscript published on 30 October 2025
*Correspondence Author(s)
Dr. Madhuri Paradesi, Associate Professor, Department of Law, Sri Padmavati Mahila Visvavidyalayam, Tirupathi (Andhra Pradesh), India. Email ID: madhuriparadesi@gmail.com
Dr. P. Jogi Naidu, Associate Professor, Damodaram Sanjivayya National Law University, Visakhapatnam (Andhra Pradesh), India. Email ID: pjoginaidu1@dsnlu.ac.in
Mr. Goriparthi. Naresh*, Assistant Professor, KL College of Law, Koneru Lakshmaiah Education Foundation, Vaddeswaram (Andhra Pradesh), India. Email ID: goriparthinaresh123@gmail.com, ORCID ID: 0009-0005-1734-0268

I. INTRODUCTION

The field of *cybersecurity is constantly evolving*. Technological advancements primarily cause the evolution of modern risks. Being more attentive is necessary to stay one step ahead of cybercriminals. In this era of digitalisation, cybersecurity has become a growing concern for both personal and business protection. Protecting computer system networks and Internet data against fraudulent activities, such as theft, phishing, Trojan horses, malware attacks, restricted data access, and damage, is known as cybersecurity. The primary aim of cybersecurity is to ensure the confidentiality of digital assets, as increasing reliance on cyberspace heightens the threat of cyber-attacks for individuals, organisations, and governments.

A. Definition of Cybercrimes

The legal framework lacks uniformity of "cyber-crimes" in any Indian laws or legislation. The term "cyber" is used in relation to information technology, computers, and other related fields. Consequently, it seems sense that "cyber-crimes" include acts involving computers, information technology, the internet, and virtual reality1. Instead of focusing on a physical body, the targets of such attacks are the corporate or personal digital entities, which consist of accumulated data and information traits that define people and organisations on Online platforms. Cybercrime impacts multiple individuals. State and non-state actors worldwide commit cybercrimes, which include financial theft, espionage, and other cross-border crimes. When cybercrimes cross national borders and involve one or more nation-states, they are referred to as cyberwarfare. "A crime involving the misuse of digital resources in cyberspace or via the internet or network networks, whether through wired or wireless communication," according to Odumesi (2014) [1], is referred to as cybercrime.

B. Types of Cybercrime

Since the global COVID-19 pandemic, people's offline-to-online behavioural patterns have undergone a significant shift. The amount of $7.1 trillion in 2022, up from $1.2 trillion in 2019, has become a lucrative target for crooks. Numerous cybercrimes are prevalent not only in India but also in other Western nations, including the United States, the United Kingdom, Germany, and Russia.

i. Phishing

Attackers employ phishing to mislead users into engaging in "the wrong thing," including clicking a malicious URL designed to deploy malware or

lead users to a dubious browser. Phishing is a method used by attackers to distribute fraudulent emails that seem to come from reputable sources. Email sources are commonly used for this purpose, with the primary objective being to illicitly acquire confidential data, including credit card details and access personal data by compromising the victim's system with malware.

ii. Ransomware

Ransomware is a constantly evolving type of virus that encrypts files on a device, rendering them unreadable, and demands payment to unlock them. These tools are intended to help people and organisations in thwarting assaults that might seriously disrupt business operations and deprive businesses of the data necessary to function and provide mission-critical services. This type of ransomware impacts pricing or exchange rates. Nowadays, ransomware developers typically demand Bitcoin payments in exchange for their malicious software. According to FBI estimates, over 623 million ransomware attacks occurred globally in 2021, and 493 million in 2022.

iii. Cyber-Pornography

Cyber pornography is termed the enactment of creating, displaying, distributing, importing, or publishing explicit or obscene materials online, particularly those that involve minors in sexual activities with adults. The term 'pornography' refers to the depiction or demonstration of sexual acts intended to elicit sexual arousal, typically through various media such as literature or films. For younger generations, it is often seen as an act of rebellion and a quick source of gratification. In comparison, older generations perceive it as a breach of moral, ethical, and cultural values.

iv. Cyberterrorism

Also known as digital terrorism, cyberterrorism involves attacks on computer systems by recognised terrorist groups with the intent to create panic, fear, or disrupt critical information systems. Examples of cyberterrorism include:

- Introducing viruses into data networks
- Hacking servers to steal confidential information
- Defacing websites to block access
- Attacking financial institutions to steal funds
- Creating widespread fear and disruption.

v. Identity-Theft

Identity theft arises when a person wrongfully acquires another person's private data, such as their phone number, birthdate, and credit card information, and uses it for deceptive purposes. It denotes the unauthorised acquisition, use, manipulation, or transfer of another person's identity, whether legal or natural, with the intention to commit, execute, or engage in deceit.

vi. Online-Stalking

Cyberstalking involves the use of the internet or other technological means to harass, follow, or make repeated unwanted attempts to approach someone. It can include behaviours such as publishing obscene material online, false accusations, defamation, teasing, or even threats. While cyberstalking is a broader term for online harassment, it often encompasses activities meant to cause emotional distress and harm to the victim.

II. CYBER LAW LEGISLATION IN INDIA: A COMPREHENSIVE OVERVIEW

A. Information Technology Act, 2000

Before the enactment of the "*Information Technology Act, 2000* (ITA 2000)" [2], India lacked a dedicated statutory framework to address emerging issues related to cybercrimes, privacy breaches, jurisdictional conflicts, and "Intellectual Property Rights" in cyberspace. In light of the swift expansion of the internet and digital technologies, the Indian government recognised the urgent need for legislation to regulate and control cybercrimes, while protecting individuals' online privacy and data security.

The Indian Parliament enacted the ITA 2000 to address challenges in the growing domains of e-commerce, e-governance, e-banking, and cybercrimes. The Act also laid down penalties and punishments for cybercriminal activities, ensuring a robust legal framework to combat digital fraud and threats. In response to the evolution of cybercrimes and the emergence of more complex cybercrimes, the ITA 2000 was amended in 2008 as per the *Information Technology Act, 2008* (ITAA 2008) [3]. This amendment introduced several new provisions to address concerns such as data protection, cyberterrorism, and the growing threats posed by new technologies, including mobile devices, cloud computing, and social media platforms.

The Indian legal framework shares similarities with the cyber laws in Europe and the United States, particularly in terms of protecting users' rights in the digital world. However, there are key differences in the application, scope, and enforcement of these laws across regions.

B. Key Provisions of the Information Technology Act, 2000

Section 65 – Tampering with Computer Source Documents This provision criminalises the deliberate destruction, concealment, or alteration of computer programs or information that are legally required to be maintained. The penalty for this offence is imprisonment for up to three years, a fine of up to ₹ two lakhs, or both. Comparison: In Europe, similar laws exist under the *EU Directive 2013/40/EU on Attacks Against Information Systems*, which criminalises illegal access to and interference with information systems, including altering, deleting, or damaging data. In the U.S., the *Computer Fraud and Abuse Act (CFAA)* [5] criminalises similar actions, imposing penalties for unauthorised access to and damage to computer systems or data.

Section 66 – Using Another Person's Password. This section addresses the fraudulent use of another individual's password, digital signature, or unique identification details. Subject to penalty or imprisonment for up to three years and/or a fine of up to 1 Lakh INR. In Europe, password theft and fraud are covered by the *General Data Protection Regulation (GDPR)* in cases involving unauthorised access to personal data. In the U.S., this would be covered under the *CFAA* and various state-level identity theft laws.

- *Section 66D – Cheating Using Computer Resources:* This provision penalises fraud committed using computer resources or communication devices, punishable by imprisonment for up to three years and/or a fine

of up to ₹ 1 lakh. Similar offences are covered under European and American cybercrime laws. The *EU Directive on Cybercrime* addresses offences related to using digital tools to commit fraud. In the U.S., the Wire Fraud Statute also extends to digital communications used for fraudulent purposes.

- *Section 66E – Publication of Private Images Without Consent:* This provision addresses the non-consensual capturing, transmission, or publication of private images or videos, specifically those of an individual's private body parts. Offenders can be charged with imprisonment for up to 3 years and a fine of up to ₹ two lakhs. Comparison: In Europe, similar offences are governed by laws under the *EU Data Protection Regulation* and individual member state laws, such as the *Revenge Pornography* laws in the UK. The U.S. has introduced various state laws criminalizing revenge porn, with penalties varying across states.
- *Section 66F – Cyber Terrorism:* This section criminalises acts that threaten the integrity, security, or sovereignty of India through cyber means, with a penalty of life imprisonment. Comparison: In Europe, cyber terrorism is addressed by the '*EU Directive 2002/58/EC* on Privacy and Electronic Communications and the *EU Directive 2013/40/EU'*. The U.S. addresses similar acts under the *Patriot Act*, focusing on cyber-attacks against critical infrastructure that threaten national security.
- *Section 67 – Child Pornography:* Any source of child pornography, whether through creating, publishing, or transmitting sexually explicit images or videos of minors, is punishable by up to seven years in prison and a fine of up to 10 Lakhs INR. Comparison: In Europe, child pornography is governed by strict laws, such as the *EU Directive 2011/93/EU*, which criminalizes child sexual abuse material. In the U.S., the *Child Online Protection Act (COPA)* and *Protect Act* provide severe penalties for such offences, with federal penalties reaching up to life imprisonment.
- *Section 69 – Government Powers to Block Websites:* This section grants the government the authority to block access to websites that may pose a threat to national security or public order. The central government may block information from public access if it deems it necessary.
- *Comparison:* In Europe, website blocking is governed by the *EU e-Privacy Directive*, which permits the removal of harmful online content. In the U.S., content regulation is more complex due to the First Amendment, which provides broader free speech protections, although certain types of content (such as child pornography) can be blocked.

III. CYBERSECURITY FRAMEWORK IN INDIA: POLICIES AND LAWS

A. Cybersecurity Legislation in the "United States of America"

The United States faces an increase in the number of cyberattacks and cybercrimes globally. Given the scale and sophistication of these threats, U.S. cybersecurity laws are complex and fragmented, with different federal agencies implementing their own cybersecurity regulations. In addition, there are sector-specific laws governing critical infrastructure, ensuring a tailored approach to cybersecurity across various industries.

B. Below are some of the key U.S. Cybersecurity Laws:

The Counterfeit Access Device and Computer Fraud and Abuse Act, 1984 (CFAA): This act primarily addresses attacks on computer systems containing sensitive information related to international trade, government data, and global e-commerce. It criminalises the unsupervised grant of access to computer systems and the misuse of information stored in such systems, making it one of the most critical pieces of legislation for regulating cybercrimes.

The Computer Security Act of *1987* established the *National Institute of Standards and Technology (NIST)*, which plays a critical role in developing security standards and ensuring their implementation across government systems. The act was designed to reduce cybercrimes by fostering cybersecurity awareness and implementing best practices. However, it does not apply to military or defence-related systems.

C. Comparison: India vs. the United States

When comparing India's cybersecurity legislation to that of the United States, there are several notable differences:

i. Legislative Frameworks

India: The "*National Cyber Security Policy, 2013* and the *National Cyber Security Strategy, 2020*" provide a strategic roadmap for national cybersecurity, but do not offer specific legal provisions for cybersecurity crimes, unlike the U.S.
U.S.: The U.S. has a highly structured and comprehensive set of laws, such as the *CFAA* and the *Computer Security Act*, that specifically address cybercrimes, data breaches, and safeguarding the vital infrastructure.

ii. Government Role and Agency Oversight

India: The Indian government has established bodies, such as the Computer Emergency Response Team (CERT-In), to handle cybersecurity incidents and implement national cybersecurity policies. However, the role of agencies in enforcing cybersecurity laws is still evolving.

U.S.In contrast, the U.S. has well-established agencies, such as the Department of Homeland Security (DHS)[6] and the Federal Bureau of Investigation (FBI), which play crucial roles in enforcing cybersecurity laws and managing national cybersecurity strategies.

iii. Private Sector Collaboration

India: The *National Cyber Security Policy* emphasises public-private sector collaboration to address cybersecurity challenges. This collaborative approach is still in its early stages of development.

U.S.In the U.S., private sector collaboration is more ingrained, with companies required to report cyber incidents to government agencies and collaborate with law enforcement to address cyber threats.

iv. Sector-Specific Laws

India: India's legal framework primarily focuses on overarching policies, lacking sector-specific laws for key industries, such as finance,

healthcare, and critical infrastructure.

U.S.: The U.S. has sector-specific cybersecurity laws that apply to various critical industries, such as the "Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the Federal Information Security Modernisation *Act (FISMA)* for government agencies."

D. Cybersecurity Laws and Regulations in the United States

i. The Homeland Security Act, 2002 (HSA)

"The *Homeland Security Act of 2002"* is a significant enactment that established the "*Department of Homeland Security" (DHS)*. This law aimed to centralise the responsibility of safeguarding the nation's critical infrastructure, including its cybersecurity. The HSA delegated authority to the recently established Homeland Security agency to develop cybersecurity standards for both public and private organisations. These guidelines are crucial in protecting sensitive government and private sector data from cyber threats.

The act also tasked the DHS with coordinating efforts between federal, state, and local agencies to develop strategies for responding to and preventing cyber-attacks. Accordingly, the act has laid the groundwork for many of the cybersecurity initiatives in the U.S., which continue to evolve as new cyber threats emerge.

ii. "The Cyber Security Research and Development Act, 2002"

The "*Cyber Security Research and Development Act of 2002"* was enacted to foster innovation and research in the field of cybersecurity. Its primary objective was to establish agencies dedicated to researching and developing solutions for preventing cyber-attacks and enhancing the nation's cyber infrastructure. This act laid the groundwork for federal institutions, such as the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST), to take on the responsibility of spearheading cybersecurity research and infrastructure improvements.

The act aims explicitly to increase investments in cybersecurity research-driven advancements to stay ahead of upcoming threats. Through this initiative, the U.S. government seeks to strengthen its technological capabilities and equip the nation with the necessary tools to defend against complex cyber threats. NSF and NIST have played vital roles in standardizing cybersecurity practices and ensuring that cutting-edge solutions are developed to safeguard the digital economy.

iii. The E-Government Act, 2002

The *E-Government Act of 2002* was a pioneering piece of enactment that provided a comprehensive framework for managing information technology within the U.S. federal government. The law not only focuses on improving the delivery of government services through electronic means but also emphasises cybersecurity requirements that federal agencies must adhere to. The act introduced specific rules for cybersecurity management, including establishing standards for protecting government data and ensuring the security of online services used by citizens. It also encourages the development of e-government projects that are secure, transparent, and easily accessible. By requiring agencies to implement proper cybersecurity measures, this act aimed to create a secure foundation for the growth of e-governance in the United States.

Over time, as cyber threats became more sophisticated, the U.S. government continued to amend this act and pass new legislation—examples of Subsequent U.S. Cybersecurity Laws.

To keep pace with the rapidly evolving disposition of digital threats, the U.S. has introduced several laws over the years to enhance its cybersecurity defences and protect critical sectors such as healthcare, finance, and energy.

E. "Federal Exchange Data Breach Notification Act, 2015"

The "*Federal Exchange Data Breach Notification Act of 2015"* focuses specifically on the healthcare sector, which handles vast amounts of sensitive personal and medical data. This act requires healthcare providers and insurers to notify patients of any data breach within sixty days of discovering the breach. Additionally, the act mandates that patients be compensated for any damages resulting from the breach. Failure to comply with these requirements can result in severe penalties. This act aims to protect the personal health information of every individual and reinforce trust in the healthcare system by ensuring that breaches are dealt with transparently and efficiently.

F.Cyber Security Enactment Act, 2014

The *Cybersecurity Information Sharing Act of 2014 was introduced to improve and modernise the United States'* cybersecurity frameworks. Some of its key objectives include:

- Developing better cybersecurity rules and regulations for both government agencies and private entities.
- Enhancing the country's cybersecurity infrastructure to ensure that critical sectors remain resilient to cyberattacks.
- Increasing awareness about the various types of cyber-attacks and educating individuals and organizations on how to mitigate risks.
- Providing support for victims of cyber-attacks and implementing preventive measures to reduce the risk of future incidents.

The act underscores the importance of continuous adaptation to evolving cyber threat landscapes and the necessity for a flexible, resilient cybersecurity strategy.

G. "Cyber Security Information Sharing Act, 2015 (CISA)"

"The *Cyber Security Information Sharing Act (CISA")* [7] was passed to promote information sharing between various federal agencies, private companies, and other stakeholders involved in cybersecurity. One of the primary objectives of this act is to facilitate the real-time provision of data about digital threats, vulnerabilities, and incidents. By encouraging the swift communication of cybersecurity challenges, the government aims to enhance the nation's collective capacity to recover from cyberattacks.

This act encourages collaboration among various sectors, particularly in

addressing cyber threats that may impact national security, the economy, or public safety. With its emphasis on information sharing, CISA aims to create a more coordinated approach to cybersecurity that benefits both private industry and government agencies alike.

The U.S. has established a comprehensive and intricate network of cybersecurity laws and regulations that address various aspects of cybersecurity, ranging from research and development to data breach notification. These laws aim to protect critical infrastructure, ensure data privacy, and provide a framework for responding to cyber-attacks.

The "*Homeland Security Act, 2002* and the *Cyber Security Research and Development Act, 2002",* laid the groundwork for federal cybersecurity efforts, while the *E-Government Act, 2002,* ensured the integration of cybersecurity into the operations of federal agencies. More recent laws, such as the "*Federal Exchange Data Breach Notification Act, 2015* and the *Cyber Security Enactment Act, 2014*, focus on specific industries and address emerging challenges in the digital age. "The *Cyber Security Information Sharing Act, 2015 (CISA)"* emphasizes collaboration and information sharing to form a more resilient cybersecurity ecosystem.

Through these comprehensive legislative efforts, the U.S. has developed a robust and evolving cybersecurity framework aimed at *protecting* its citizens, businesses, and essential infrastructure from cyber threats. However, as cyber-attacks continue to grow in sophistication, ongoing updates to these laws will be instrumental in maintaining national security in an increasingly digital world.

IV. UNITED KINGDOM'S CYBERSECURITY LAWS

The *UK* has established a robust legislative framework to address cybersecurity, focusing on data protection, network security, and implementing effective cybersecurity practices across various sectors.

A. Data Protection Act, 2018 (DPA, 2018)

The *Data Protection Act, 2018 [4]* is the cornerstone of data protection law in the UK, mirroring the EU's General Data Protection Regulation (GDPR) in terms of its objectives and scope. The act regulates the collection, storage, and management of personal data by government bodies and private organizations. It ensures that individuals' personal data is processed securely, with stringent penalties for non-compliance. Non-compliant organisations that fail to adhere to the provisions of the DPA, 2018, may incur significant fines, reaching up to € 17.5 million or 4% of their global annual turnover, whichever amount is higher.

B. UK-GDPR (United Kingdom Data Protection Regulation)

The *UK-GDPR [8]* is essentially a continuation of the EU-GDPR, but adapted to the UK's legal framework following Brexit. It imposes stringent requirements on businesses to safeguard the personal information of UK citizens, with a clear focus on ensuring transparency, accountability, and security in the processing of data. Penalty for Non-Compliance: Non-compliance with the UK GDPR can result in substantial fines, up to £20 million or 4% of the organisation's annual turnover, whichever is the greater amount.

C. Network and Information System (NIS) Regulations, 2018

The *NIS Regulations, 2018 [9]* are a key legislative development in the UK, transposed from the EU's NIS Directive. These regulations focus on the security of network and information systems that are critical to the functioning of the economy and society, such as energy, transport, healthcare, and finance.

a. The act requires organizations to implement robust security measures to protect their network and information systems from cyber threats, and to notify the authorities in case of significant security incidents.

b. Penalty for Non-Compliance: Penalties for failure to comply with the NIS Regulations include fines of up to 19 million pounds or 4% of global yearly capital.

V. CONCLUSION

The increasing digitalisation of economies and the rise in cyber threats have made cybersecurity a critical concern for nations worldwide. Each country, although facing similar challenges, has crafted unique legal frameworks to address cybersecurity threats and affirm the defence of digital infrastructure and citizens' data.

The United States has a robust yet fragmented approach to cybersecurity, characterised by a multitude of sector-specific laws and a stronger emphasis on information sharing between the public and private sectors. The U.S. has established key legislation, such as the "*Cybersecurity Information Sharing Act (CISA)* and *the Federal Exchange Data Breach Notification Act, which aim to enhance the country's collective defence* against cyber threats. However, the diverse and decentralised nature of U.S. cybersecurity laws can sometimes lead to challenges in coordination and enforcement. The United Kingdom offers a more unified and comprehensive approach to cybersecurity, particularly through its adherence to the UK GDPR and the *Network and Information Systems (NIS) Regulations*. The UK's focus on personal data protection, alongside its emphasis on securing critical infrastructure, demonstrates a commitment to striking a balance between the need for national security and the right to individual privacy. The UK's legal framework also reflects its intense collaboration with international partners, particularly following Brexit, to safeguard its digital landscape. India, while still in the process of strengthening its cybersecurity framework, has made notable strides through the *Information Technology Act, 2000* and the *National Cyber Security Policy, 2013*. However, challenges remain in terms of resource allocation, enforcement, and adapting to the Fluid character of cyber threats. India's growing digital economy necessitates the development of comprehensive and enforceable laws to effectively address the complexity of modern cyber threats. In all three countries, data protection and privacy remain central to their cybersecurity laws. However, their regulatory approaches differ significantly. The UK's stringent penalty mechanisms under the *UK GDPR and the Data Protection Act 2018 [10]* reflect its strong commitment to data security. In contrast, the U.S. focuses more on sector-specific regulations and information sharing [11], while India is

gradually advancing toward a more cohesive data protection framework.

Ultimately, all three countries have made significant progress in addressing cyber threats, raising public awareness, and fostering international cooperation. Efforts to combat cyber threats have advanced, alongside initiatives aimed at increasing public awareness and strengthening global collaboration to tackle these challenges more effectively. The continuous adaptability of laws to recent and emerging technologies is crucial for enhancing the effectiveness of these cybersecurity frameworks [12]. These nations must collaborate and share knowledge in combating the evolving threat landscape, finding a balance between protecting everyone's privacy rights and ensuring national security. As technology continues to emerge, so too must the legal frameworks that protect our digital future. The ongoing refinement and strengthening of cybersecurity laws in the U.S., UK, and India are essential to safeguarding both digital infrastructures and personal data in an increasingly connected world.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it was conducted without any external influence.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors' Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Ali, A., Shah, M., Foster, M., & Alraja, M. N. (2025). Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country. Computers, 14(2), 38. DOI: https://doi.org/10.3390/computers14020038
2. Exposing the Impact of GenAI for Cybercrime: An Investigation into the Dark Side. Truong, Luu, Binny M. Samuel. (2025). arXiv preprint. https://arxiv.org/abs/2505.23733
3. Cryptologic Techniques and Associated Risks in Public and Private Security: An Italian and European Union Perspective with an Overview of the Current Legal Framework. Zana Kudriasova. (2025). arXiv preprint. https://arxiv.org/abs/2505.08650
4. AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. International Journal of Law and Policy, 2(5), 28–36. DOI: https://doi.org/10.59022/ijlp.191
5. Transformation of Crimes (Cybercrimes) in the Digital Age. AllahRakha, N. (2024). International Journal of Law and Policy, 2(2). DOI: https://doi.org/10.59022/ijlp.156
6. Some New Challenges of Cybercrime and the Reason for Its Outdated Regulations. Anri Nishnianidze. (2023). European Scientific Journal, 19(39), 92. DOI: https://doi.org/10.19044/esj.2023.v19n39p92
7. United States Congress. (2015). Cybersecurity Information Sharing Act (CISA), 2015. Public Law 114-113. https://www.congress.gov
8. European Parliament and Council. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu
9. European Parliament and Council. (2016). Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive). Official Journal of the European Union, L194, 1–30. https://eur-lex.europa.eu
10. United Kingdom Parliament. (2018). Data Protection Act, 2018. c.12. https://www.legislation.gov.uk/ukpga/2018/12
11. United Kingdom Parliament. (2018). Network and Informatics Data Action Systems Regulations, 2018. SI 2018/506. https://www.legislation.gov.uk/uksi/2018/506
12. Federal Bureau of Investigation (FBI). (2022). Internet Crime Report 2022. Internet Crime Complaint Centre (IC3). https://www.ic3.gov

AUTHOR'S PROFILE

Dr. Madhuri Paradesi is currently an Associate Professor in the Department of Law at Sri Padmavati Mahila Visvavidyalayam, Tirupati. She specializes in Intellectual Property Rights and has an experience of 21 years in teaching and research. She has been awarded four PhD degrees and is currently guiding two research scholars. She has published extensively in SCOPUS-indexed and UGC-CARE-listed journals. Her research spans diverse areas, reflecting a commitment to advancing knowledge, fostering academic excellence, and making meaningful contributions to the academic community through teaching, mentorship, and scholarly engagement.

Dr. P. Jogi Naidu is currently working as an Associate Professor at Damodaram Sanjivayya National Law University, Visakhapatnam. Specializes in Air and Space Law and has over 9 years of experience in teaching and research. He is currently pursuing an LLD in Space Law and completed a PhD on "Legal Dimensions of Loss of Life or Property during Air Travel and the Scope of Compensation in India – A Critical Analysis" in 2023. He has also participated in numerous national and international research projects. His notable projects include studies on Commercial Courts in South India and the Tele-Law Program for Access to Justice, in collaboration with the Ministry of Law and Justice. Dr Naidu has authored articles in SCOPUS-indexed and UGC-CARE journals, covering topics such as aviation, space law, digital banking, and environmental law. He has also contributed as a resource person, editor, and conference chair, with active involvement in curriculum development and capacity-building initiatives.

Mr. Goriparthi. Naresh, currently working as an Assistant Professor at the College of Law, KL University, Vaddeswaram. specializes in Corporate and Financial Laws. He has also served as Field Investigator for the ICSSR-sponsored project "Integration of Digital Technologies for Transforming Rural Occupational and Livelihood Diversification Strategies in South India." He is currently involved in research in the field of Anti-Dumping laws and Insolvency and Bankruptcy laws.