Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
( Fulfilled Suggests Parametres of UGC by IJMER)
Volume:14, Issue:7(2), July, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

# CYBER SECURITY ACT AND DIGITAL PRIVACY: A CRITICAL STUDY IN INDIAN PERSPECTIVE

**[1]Dr. Apara Prajapat and [2]Dr. Rakesh Damor**
[1]Asst. Prof., Dr. Nagendra Singh Law College, Banswara (Raj.) Affiliated to Dr.Bhimrao Ambedkar Law University, Jaipur
[2]Dean, College of Law, Govind Guru Tribal University, Banswara (Raj.)

## Abstract

In the current digital age, when the entire society is becoming dependent on information technology, cyber security and digital privacy have emerged as two important topics that are not limited to technical concerns but are also directly linked to civil rights, national security, and democratic values. This research paper analyzes the state of cyber security in India, constitutional recognition of digital privacy, existing legal framework, and level of awareness of citizens. This research mainly makes it clear through legal references such as the Information Technology Act, 2000, CERT-In, and Puttaswamy v. Union of India (2017) that India has a legal system to deal with cybercrimes and data breaches, but it is not adequate in accordance with the nature and intensity of the current digital threat. The research also found that despite legislative efforts such as the Digital Personal Data Protection Bill, 2023, no clear and effective data protection law has been implemented in India till now. The research indicates that rising incidence of cybercrimes, lack of digital literacy, complexity of legal systems, and imbalance between surveillance versus privacy are the major problems facing India. To address these problems, the research proposes several corrective measures such as enactment of strong data protection laws, speedy investigation of cybercrimes, cyber security education for citizens, and promotion of technological self-reliance.

**Key Words:** Cyber Security, Digital Privacy, Right to Privacy, Digital Literacy, Technological Self-Reliance

## Meaning and Importance of Cyber Security

Cyber security refers to the technical, legal and policy measures that are implemented to protect computer systems, networks, mobile devices, cloud services and digitally protected data from unauthorized access, destruction, tampering and cyber-attacks. Its basic objective is to ensure confidentiality, integrity and availability of information, which is commonly known as the "CIA Triad". In the present era when every section of the society is becoming dependent on digital means, cyber security has become an integral part of the social and legal structure rather than just a technical measure.
The need for cyber security in India is increasing day by day as the use of digital transactions, online banking, e-governance and mobile applications is increasing rapidly here. Cyber criminals try to access sensitive information such as banking passwords, identity cards, mobile data, and even biometric information, which can pose a serious threat to the economic and social security of an individual. For example, disputes related to the security of Aadhaar card data, debit card cloning and phishing cases have seen a huge increase.

In addition, cyber security has also become extremely important from the point of view of national security. Today, defense systems, intelligence agencies and communication media are digitally connected, which can be harmed by cyber-attacks. Incidents of cyber-attacks on Indian institutions by China and other countries clearly show this danger. To weaken the strategic capabilities of a nation, not conventional war, but 'cyber war' is now being resorted to.

Cyber security is also of great importance from a business point of view. Institutions like banking, insurance, e-commerce and social media depend on customer data. If the data of these institutions is leaked or the services are hacked, not only financial loss occurs but the credibility of the institution also comes under question. For example, in 2016, information of millions of debit cards of State Bank of India was leaked, which raised serious questions on the cyber security system of the banking system.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
( Fulfilled Suggests Parametres of UGC by IJMER)
Volume:14, Issue:7(2), July, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

Protection of digital privacy has today become a question of human and constitutional rights. The spread of fake profiles, morphed photographs and pornographic content on social media platforms has a negative impact on the privacy and mental health of women and adolescents. The courts also recognized privacy as a fundamental right in the case of 'Puttaswamy vs Union of India (2017)', which makes it clear that cyber security is not limited to data but is also a subject related to civil rights.

The major cyber security law in India at present is the Information Technology Act, 2000 (IT Act, 2000), under which hacking, data theft, transmission of pornographic material, phishing, identity theft, etc. have been categorized as crimes. Apart from this, the government has established agencies like CERT-In which monitor and respond to cyber incidents. However, no clear and comprehensive "Data Protection Act" has been implemented in India so far, which clearly shows the weakness towards the protection of digital privacy.

In today's time, cyber-attacks like Ransomware, Phishing, Malware, and DDoS have become common. These not only cause personal loss, but also put institutional and national security at risk. In such a situation, cyber security is not only the responsibility of technical experts, but has become the collective responsibility of every citizen, student, government official, and corporate organization.

**Concept of Digital Privacy**

Digital privacy is the right under which a person gets the freedom to decide for himself when, how and to what extent his personal information should be shared with others. In the digital age, when most of the activities of a person – such as communication, transactions, social media use, health records, travel details, location data and even biometric information – are stored on electronic platforms, the protection of digital privacy becomes extremely important.

Digital privacy is not just a matter of technical security, but it is an issue related to the dignity of the individual, self-determination and fundamental rights granted by the Constitution. This right guarantees every citizen that no government or private institution can use, analyze or disseminate his personal information without his consent. The collection and use of user data by social media companies, app developers and e-commerce platforms has become a common practice today, which is done many times without explicit consent. This puts the user's digital freedom at risk.

The foundation of constitutional recognition of digital privacy in India was laid in the landmark Supreme Court judgment in Justice K. S. Puttaswamy v. Union of India (2017) in which a nine-judge Constitutional Bench unanimously held that the right to privacy is an integral part of the fundamental right to life and personal liberty under Article 21 of the Indian Constitution. This judgment provided a constitutional safeguard to digital privacy and placed an obligation on the government and private entities to store citizens' information in a transparent, secure and consent-based manner.

Another important effort towards protecting digital privacy is the "Digital Personal Data Protection Bill, 2023", which is still pending as a bill. The bill provides clear provisions for the responsibility of data processors and collectors, user consent, limits on data storage and penalties for misuse. The bill is considered an important step towards establishing a robust data protection system in India in line with the European Union's General Data Protection Regulation (GDPR). However, many challenges related to digital privacy still exist in India. Most citizens do not know what data the apps or websites they are using are accessing and for what purpose. In addition, personal data is illegally collected through free Wi-Fi, online lottery, mobile games, etc., which threatens the privacy of users. In this context, it is also worth mentioning that protecting digital privacy is not only the responsibility of the government, but it is also the responsibility of citizens to use digital platforms with caution and discretion. Citizens should take measures at their own level such as reading the permission policy while installing a mobile app, avoiding sharing personal information on social media and using a secure password.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
( Fulfilled Suggests Parametres of UGC by IJMER)
Volume:14, Issue:7(2), July, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

**Cyber Security Laws in India**

The Information Technology Act, 2000 has been implemented primarily to control cybercrimes and illegal activities on digital platforms in India. This Act provides legal validity to electronic records, digital signatures, cybercrime and e-governance. Section 43 of this Act considers acts such as unauthorized access, data damage, virus attacks as crimes. Computer hacking has been declared a punishable offense under Section 66, while crimes such as identity theft have been defined in Section 66C and forgery in Section 66D. Apart from this, electronic publication of pornographic material has also been categorized as a crime in Section 67. This Act is the basic cyber law of India, but in view of the current technological development, there is a constant need to amend it.

In addition, there are some provisions under the Indian Penal Code, 1860 (IPC) which apply to cybercrimes. For example, sections 419 and 420 criminalize fraud, identity theft, and electronic fraud. These sections of the IPC complement the Information Technology Act, especially when the nature of the crimes is complex and multifaceted.

The Government of India has set up CERT-In (Computer Emergency Response Team – India) to monitor and respond to cyber security, which monitors, alerts, and responds to cyber threats, attacks, and data breaches at the national level. CERT-In issues advisories to various government and private entities from time to time and provides assistance in technical analysis of cyber-attacks. This institution is considered to be the main pillar of the cyber security system in India.

The Digital Personal Data Protection Bill, 2023 proposed by the Government of India is another important legislative effort, which aims to ensure the protection of personal data of citizens. This bill clarifies that no institution or service provider can collect, analyze or distribute user data without their consent. The bill also provides for the establishment of new structures such as data processor, data fiduciary and data protection board. Although this bill has not yet been passed as an Act, it is still considered a revolutionary step towards the protection of digital privacy in India.

In addition, the government has made efforts to increase monitoring and accountability on social media and digital platforms through the IT Rules, 2021. According to these rules, social media companies will have to appoint a grievance officer, resolve the user's complaint within the stipulated time, and provide information about the first source if required. These rules may prove helpful in controlling cybercrime and the spread of misinformation, but there is also widespread debate about its effects on the right to privacy. Cyber security laws in India are constantly evolving, but many improvements are still needed given the pace of technological development. Only a coordinated, transparent and strong legal framework can truly protect citizens' data and digital freedom.

Current Issues and Challenges in Cyber Security and Digital Privacy
India faces a number of serious challenges in the field of cyber security and digital privacy, which create complexities not only from a technical perspective but also at the legal, social, and administrative levels. Despite the rapid expansion of the digital system, India does not yet have a complete and consistent data protection law. Although a “Digital Personal Data Protection Bill” has been proposed, it has not yet been passed as an Act. This makes it clear that the security of citizens' personal information is not completely assured, especially when big tech companies and online services are collecting users' data in an uncontrolled manner.

Another major challenge is the increasing number of cybercrimes and the delay in their investigation. Indian law enforcement agencies and police departments still lack technical resources and expertise to investigate cybercrimes. Most police stations lack cyber experts, making it difficult for victims to get justice. Also, many times victims hesitate to lodge their complaints themselves, especially when the matter is related to social media harassment, data leaks or pornographic content.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
( Fulfilled Suggests Parametres of UGC by IJMER)
Volume:14, Issue:7(2), July, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

Lack of digital awareness among ordinary citizens is also a serious problem. Many users do not know what data is being shared on mobile applications or websites, or what kind of permissions are being given to them. Cyber criminals easily access people's data through social media, free Wi-Fi, fake links, and suspicious apps. This situation is not only dangerous for individual privacy, but is risky for the entire society.

Also, the irresponsibility and lack of transparency of social media companies and internet service providers has also become a threat to digital privacy. These companies often present their terms of service and privacy policy in complex language, due to which common users are unable to understand it. Additionally, many times foreign companies transfer Indian data abroad, making it outside the scope of Indian law. This causes serious damage to data security and user freedom.

The lack of basic cyber security infrastructure in India is also a major challenge. Rural and backward areas have neither adequate internet literacy, nor strong network security systems. Small businesses and startups do not have enough resources to spend on cyber security, making them more vulnerable to hacking, ransom ware and malware.

Finally, it is also a challenge that striking a balance between privacy versus national security is a difficult task. Governments sometimes increase digital surveillance in the name of security, which encroaches on privacy. In recent years, fears of the use of spyware like "Pegasus" in India have further intensified the debate whether it is justified to infringe on the digital freedom of citizens in the name of surveillance and security?

**Solutions and Remedial Measures**

**1. Creation and implementation of a comprehensive and robust data protection law**
India is in dire need of a comprehensive and clear data protection law, which sets clear guidelines and responsibilities for the protection of personal data of citizens. The "Digital Personal Data Protection Bill, 2023" is an important effort in this direction, which regulates the processes related to data collection, processing, transfer and destruction. Under this law, the user should have the right to demand information, permission and deletion of his data (Right to be Forgotten). Also, it is necessary to make government and private entities transparent and accountable. If this law is implemented effectively, India can move towards a data-secure nation.

**2. Quick and expert investigation system for cyber crimes**
At present, the capacity of our police and judicial system is inadequate in proportion to the increasing number of cyber-crimes. Therefore, it should be mandatory to establish specialized cyber-crime units in every district. Also, investigating officers should be trained in digital forensics, data analysis, and legal sections of the IT Act. Establishment of "fast track cyber courts" in courts will ensure speedy justice to victims. An effective investigation mechanism will not only prevent crime but also instill a sense of security in society by ensuring strict punishment to the criminals.

**3. National Mission on Digital Education and Cyber Literacy**
India's vast population is now connected to the Internet, but the level of digital literacy is still low. Especially in rural and less-educated areas, people are using the Internet, but are not aware of the basic principles of security such as strong passwords, two-factor authentication, protection from phishing, etc. The government should organize cyber security awareness programs at schools, colleges and panchayat levels. This effort will not only increase security, but will also make citizens responsible digital consumers.

**4. Strengthening technological self-reliance and cyber infrastructure**
India should move towards technological self-reliance by breaking away from excessive dependence on foreign tech companies. For this, the government should invest in developing secure cloud services, data centers and encryption technologies in the country under the 'Make in India' campaign. Also, the public and private sectors should collaborate in

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
( Fulfilled Suggests Parametres of UGC by IJMER)
Volume:14, Issue:7(2), July, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

R&D for cyber security. Citizens' data should be stored and protected within India's borders by encouraging data localization policy.

**5. Making social media and digital companies accountable**

Social media platforms, app developers, and online services need to be transparent, ethical, and accountable. While some initiatives have been taken in the IT Rules, 2021, these companies should still be made to follow strict rules such as publishing data transparency reports, removing fake accounts, and timely resolution of user complaints. Commercial use of data without user consent should be prohibited.

**6. Striking a balance between privacy and national security**

It is essential for the government to strike a balance between the privacy of citizens and the security of the country. Surveillance mechanisms are necessary, but they must be kept clear and under judicial control, so that any kind of digital dictatorship can be avoided. After the Supreme Court declared privacy as a fundamental right, it is now the responsibility of the government to establish a clear legal framework for digital surveillance, which has transparency and accountability.

**7. Citizen Participation and Personal Vigilance**

Finally, citizens too must understand that cyber security is not just the responsibility of the government but also the moral duty of every user. Personal vigilance – such as careful use of public networks, avoiding sharing confidential information, and prompt reporting of cyber-crime – is essential. Only when society becomes aware, digital security will become a reality.

**Conclusion**

As the global society undergoes a digital revolution in the 21st century, cyber security and digital privacy are no longer limited to technical concerns but have become fundamental to national security, democratic governance, civil liberties, social trust, and economic stability. The Internet and digital platforms have provided convenience, efficiency, and speed, but have also posed serious challenges such as cybercrime, data breaches, online fraud, and privacy violations.

India has experienced rapid digital growth — UPI, Digital India, Aadhaar, mobile internet, and other technologies have digitally connected people from rural to urban areas. But the development of cyber security infrastructure and legal framework has not been robust enough to match this rapid expansion. Laws such as the Information Technology Act, 2000 are now outdated in many ways and are not fully capable of dealing with today's sophisticated cybercrimes. The legislative framework related to data protection is still at the proposal stage, leaving citizens' sensitive information unsecured across various platforms.

Digital privacy, which is a constitutional right, is today under constant threat under pressure from tech companies, social media platforms and even government surveillance systems. Identity theft, commercial use of personal information and automated algorithm-based surveillance raise questions about the freedom and dignity of users. Despite the Supreme Court declaring privacy as a fundamental right in Puttaswamy vs Union of India case, the lack of the required institutional framework for its full protection is clearly felt.

The research clearly revealed that India will have to work in parallel on many fronts to become stronger in this area. The creation and implementation of an effective data protection law should be the first step. Along with this, technically trained cyber police force, cyber courts and admissibility of digital evidence will have to be ensured for quick investigation and prosecution of cyber-crimes. It is also necessary that the government and technology providers make citizens aware of digital rights and risks so that they can become alert, responsible and empowered consumers. India must also move towards becoming technically self-reliant — such as data localization, development of indigenous cloud services, and investment in cyber security research. Along with this, there must be a stringent regulatory framework for social media and apps so that they use citizens' information in a transparent and ethical manner. The government must also bring transparency in the functioning of surveillance mechanisms so that a healthy balance between privacy and national security can be maintained.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
( Fulfilled Suggests Parametres of UGC by IJMER)
Volume:14, Issue:7(2), July, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

Finally, it can be said that cyber security and protecting digital privacy is not just the responsibility of the government or the law, but it is the shared responsibility of all stakeholders — citizens, institutions, technology companies, and the administration. No technological or legal measure can be fully successful unless every citizen is digitally empowered, aware, and conscious. Hence, India must develop an inclusive, responsive, and rights-sensitive cyber environment where technology is used only for convenience and development — not for surveillance and control. This will be a true and lasting step towards a safe, free, and democratic digital India.

**References**

1) Ministry of Electronics and Information Technology. (2000). *Information Technology Act, 2000*. Government of India. Retrieved from https://www.meity.gov.in
2) Supreme Court of India. (2017). *Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* (Writ Petition (Civil) No. 494 of 2012).
3) CERT-In. (2022). *Cyber Security Guidelines and Advisories*. Retrieved from https://www.cert-in.org.in
4) Ministry of Electronics and IT. (2023). *The Digital Personal Data Protection Bill, 2023*. Government of India. Retrieved from https://www.meity.gov.in/data-protection-framework
5) Singh, R. (2021). *Cyber Laws in India: A Critical Analysis*. New Delhi: Universal Law Publishing.
6) Sharma, V. (2020). *Privacy in the Digital Age: Legal and Policy Perspectives*. Journal of Cyber Law and Governance, 5(2), 45–61.
7) Kapoor, A. (2022). *Cyber Security in India: Challenges and Emerging Trends*. Indian Journal of Information Security, 8(1), 25–38.
8) Internet Freedom Foundation. (2023). *Pegasus Spyware Controversy and Data Privacy*. Retrieved from https://internetfreedom.in