IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

Spyware Attacks and Digital Surveillance: Emerging Legal Challenges in India

Pushparani
1st Year LL.M (CBCS) Student
School of Excellence in Law, Chennai, The Tamil Nadu
Dr. Ambedkar law University, Chennai
pushra112000@gmail.com

Abstract: *In this modernized digital era, the technological developments have greatly enhanced economic growth, governance and communication. However, the exact technologies have also introduced new risks and threads to facing cyber security and privacy. Globally including in India, Spyware attacks and Digital surveillance have grown to be serious issues. Spyware is one type of malicious software. It secretly gathers people's personals data without their knowledge or consent. Our government also use the surveillance technologies for national security and crime prevention. At the same time the excessive of uncontrolled surveillance can threaten the fundamental rights such as privacy and freedom of expression. This article explores the idea of spyware attacks and digital surveillance, how they affect people's rights and the legal challenges faced by India in regulating these technologies. It also examines India's current legal system and suggests reforms to ensure a balance between national security and individual privacy.*

Keywords: Spyware, Digital surveillance, Fundamental rights, Privacy, Pegasus

I. INTRODUCTION

The extreme growth of digital technology was the important transformation of modern society. In the modern era, communication and exchange of information with the help of smart phones, computers and internet service and also these are the essential tools to carry out the information. However, this increasing digital technology at the same time increasing the cyber threads. Cyber threads is a risk factor like hacking, data breaches and spyware attacks.

Spyware is one of the malicious software. It designed to collect information and monitor the user's device secretely. It also record keystrokes, access personal messages, track browsing history, and even activate cameras and microphones without knowledge of the user. In recent years, Spyware have become more advanced and technologically developed. It is difficult to detect.

In India, Spyware attacks and digital surveillance gained huge attention after allegation regarding the use of spyware like Pegasus. It monitor the Journalist, Activists and Political leaders. After these incident raise serious legal and constitution questions like Privacy, Accountability and the limits of government surveillance. Whatever it is surveillance may be necessary for national security. But illegitimate surveillance threaten democratic values and the Fundamental rights. Therefore, India faces significant legal challenges in controlling the Spyware attacks and Digital surveillance and also protecting both security and civil liberties.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

II. CONCEPT OF SPYWARE AND DIGITAL SURVEILLANCE

Spyware is a software code or program. [1]This is a type of malicious software, installed without the user content is capable of regarding every keystroke and surfing history and sharing the same hackers and other interested third parties.[2]

Spyware is one of the cyber attack methods. Attackers use various types of spyware to infect users computers and devices. Some of the most commonly used types of spyware include:

- System Monitors Adware
- Infostealer
- Keyloggers
- Rootkits
- Red shell
- Tracking Cookies
- Trajon Horse Virus

Common problems that spyware can result in include data theft, Identity fraud, device damage and processing disruption.[3]

Digital surveillance include the use of technology to monitor, track and analyze activities within the virtual space. This can include observing online communications, tracking financial transactions, monitoring social media platforms, or investigating breaches of data security.

The reason for employing digital surveillance services depending on the situation and the individuals involved,

- Protecting High-Net-Worth individuals
- Corporate espionage and data breaches
- Employee misconduct
- Online harassment and Cyber stalking
- Family and child safety.

In all these scenerios, digital surveillance goes beyond simply tracking activity – it provides actionable intelligence that can be used to prevent harm, resolve disputes or address legal issues.[4]

Governments and law enforcement agencies often use of surveillance tools to detect crimes, prevent terrorism, and maintain National security. Method of digital surveillance include phone tapping, Internet monitoring, CCTV and facial recognition, Data interpretation, location tracking.

III. LEGAL FRAMEWORK GOVERNING SURVEILLANCE IN INDIA:

3.1 The Information Technology Act, 2000:

The Information Technology Act, 2000: the Information Technology Act (IT Act) serves as the primary legislation governing various aspects electronic transactions and digital communication in India.

- **Section 69 of the IT Act**,

Power to issue directions for interception or monitoring or decryption of any information through any computer resource[5].

---

[1] Dave Chatterjee, cybersecurity readiness A Holistic and High Performance approach (SAGE Publications,2021)

[2] Dr Kutub Thakur, Dr Al-Sakib Khan Pathan, Cyber security fundamental A Real world perspective 85 (CRC Press, First edition 2020)

[3] Fortinet, what is spyware, https://share.google/DBk5ZgOrX2SzYx40m (11.50 AM)

[4] Paul Hawkes, Digital surveillance explained, Research Associates (2024), https:researchassociates.com/digital-surveillance-explained (12.32 PM)

[5] The Information technology act, 2000 (Act No, 21 of 2000), S.69.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

It authorizes the government to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in a computer resource in a computer resource in the interest of national security, public order, or for the prevention of offences.

- **Section 69A of the IT Act**,

Power to issue directions for blocking for public access of any information through any computer resource[6].
It empowers the government to block public access to online content where it is deemed necessary in the interest of sovereignty and integrity of India.

- **Section 72 of the IT Act,**

Penalty for Breach of confidentiality and privacy[7].
This section stated imposes penalties for unauthorized disclosure of information obtained through lawful access, thereby aiming to protect confidentiality and prevent misuse of data, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.
However, The Information Technology Act does not mentioned specifically about spyware. The act also not to provide any strong protection against misuse of surveillance powers.

3.2 Indian Telegraph Act,1885

- **Section 5(2) of the Indian Telegraph Act[8],**

Grants the power for government to intercept communication public emergencies or in the interest of public safety.
This Indian Telegraph Act also often used to authorize the power for government in phone tapping.

3.3 Constitutional Provisions

Right to privacy as a Fundamental Right

- **Article 21 of the Indian Constitution[9]** ,

Guarantees the right to life and personal liberty, a right that the Indian judiciary has interpreted to include the right to privacy.
In the landmark case Justice K.S.Puttasawamy (Retd.) v. Union of India,[10] the Indian Supreme court affirmed the fundamental right to privacy as an intrinsic part of the right to life and personal liberty protected under Article 21.
The Court held that any surveillance measures become legality, necessity, proportionality and this three conditions become satisfied.
This famous judgment plays a major role in regulating the government surveillance practices.

3.4 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016[11]

The Aadhaar Act was enacted to provide a unique identity number, that was called as Aadhaar, to residents of India. It contains provisions pertaining to the collection, storage, and use of biometric and demographic information. The Act also includes provisions for the protection of individuals privacy and places restriction on the sharing of Aadhaar related information.

3.5 Digital Personal Data Protection Act,2023[12]

---

[6] The Information technology act, 2000 (Act No, 21 of 2000), S.69 A.
[7] The Information technology act, 2000 (Act No, 21 of 2000), S.70.
[8] Indian Telegraph act, 1885 (Act No, 13 of 1885), S.5(2).
[9] Constitution of India,1950
[10] Justice K.S Puttaswamy (Retd) v. Union of India, Writ Petition (Civil) No. 494 of 2012, Supreme Court of India (2017)
[11] The Aadhar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) act,2016 (Act 18 of 2016)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

India recently enacted the new legislation that is Digital Personal Data Protection Act,2023. In this act is to regulate the collection and processing of personal data. This act main aim is to protect data privacy. So critics have lambasted that it has given too many exemptions to the state under the guise of national security to confer broad powers of surveillance.[13]

IV. EMERGING LEGAL CHALLENGES IN INDIA

Lack of specific legislation on Spyware:

India does not have any separate law to regulate the Spyware technologies. The Information Technology Act is a major act deals the cyber related problem. In that act has not exactly mentioned the Spyware, creating a legal gap.

Lack of Transparency and Accountability:

Surveillance activities are often secretive with limited pubic disclosure. The legal challenges in transparency and accountability, lack of clarity regarding who is being watched, There is no strong system to question the misuse power, inadequate system of accountability.

Risk of Misuse of Surveillance:

Pegasus spyware and other similar t+ools sparkled worries, that surveillance may be used against like Journalist, Activists, Political parties. This suppose to creates a serious threat to democracy and rule of law.

Weak Data Protection Safeguards:

Inadequate data security measures despite to Digital Personal Data Protection act, being passed in India. The legal challenge is to weakens protection against surveillance misuse.

Technological Advancement vs Legal Framework:

Spyware technologies are evolving rapidly, incorporating sophisticated features such as Zero click attacks, encrypted communication interception, and remote device control.

Technological improvement faster and advancement but laws are outdated making regulation is difficult.

Risk of misuse of Surveillance Powers:

The Government uses surveillance for security purposes, but the excessive surveillance may violate civil liberties.

V. SUGGESTION

a) India must introduce a clear and dedicating law regulating spyware technologies and digital surveillance. While the cyber crime existing Information Technology Act,2000 does not covered and not address advanced spyware threads.
b) The Digital Personal Data Protection Act,2023 should be strengthen the mechanisms and to ensure strong protection of personal data and limit excessive government access to citizen's information.
c) A specialized regulatory authority should monitor surveillance practices and to ensure the transparency and accountability.
d) Government authorities and agencies should follow legal procedures before using surveillance technologies and their duty to ensuring compliances with constitutional safeguards.
e) Government institution and private organization must enhance the cyber security infrastructure and preventing spyware attacks

[12] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023)

[13] State Surveillance And Privacy Rights: Legal Frameworks And Challenges In India - Data Protection - India https://www.mondaq.com/india/data-protection/1656884/state-surveillance-and-privacy-rights-legal-frameworks-and-challenges-in-india#:~:text=Law%20Firm%20industries-,These%20permit%20real%2Dtime%20surveillance%20of%20phone%20calls%2C%20emails%2C,vulnerable%20to%20exercise%20of%20misuse.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

f) Government must strengthen the protection of fundamental rights and ensuring that privacy and civil liberties are not violated.

g) Government must create committee and the committee should increase public awareness on digital security to educated citizens about digital privacy safe to use internet practices and methods to prevent spyware infections.

VI. CONCLUSION

Now a days the modern digital world, Spyware attacks and Digital Surveillance are increasing rapidly. While these tools may help the government to prevent the combat crime and maintain the national security. But the government misuse the power it can seriously affect the privacy and freedom of individual. The present legal framework in India, the Information Technology Act, 2000 is lack comprehension to deals with advanced spyware technologies. The Recognition of the right to privacy in Justice K.S Puttaswamy (Retd) v. Union of India has created an important constitutional safeguard yet stronger legislative and institutional mechanisms are necessary. Surveillance power run the risk of being abused, without clear laws and effective oversight.

Therefore, India must develop a clear and strong legal framework that protects both the individuals rights and national security. A Proper balance of surveillance and privacy is required to ensure Justice, Transparency and the protection Democratic values.

REFERENCES

[1]. Dave Chatterjee, cybersecurity readiness A Holistic and High Performance approach (SAGE Publications,2021)
[2]. Dr Kutub Thakur, Dr AI-Sakib Khan Pathan, Cyber security fundamental A Real world perspective 85 (CRC Press, First edition 2020)
[3]. Fortinet, what is spyware, https://share.google/DBk5ZgOrX2SzYx40m0
[4]. Paul Hawkes, Digital surveillance explained, Research Associates (2024). https:researchassociates.com/digital-surveillance-explained.
[5]. Constitution of India,1950.
[6]. Justice K.S Puttaswamy (Retd) v. Union of India, Writ Petition (Civil) No. 494 of 2012, Supreme Court of India (2017)
[7]. The Aadhar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) act,2016.
[8]. The Digital Personal Data Protection Act, 2023.
[9]. The Information technology act, 2000.
[10]. The Information technology act, 2000.
[11]. The Information technology act, 2000.
[12]. Indian Telegraph act,1885.