Surveillance Laws in India and Privacy

Why in News

Recently, a global collaborative investigative effort has revealed that, at least 300 **individuals in India, were potentially identified for targeted surveillance** using sophisticated **spyware called** <u>Pegasus</u>. However, the government has claimed that all interception in India takes place lawfully.

- Communication surveillance in India takes place primarily under two laws the Telegraph Act, 1885 and the Information Technology Act, 2000.
- While the Telegraph Act deals with interception of calls, the IT Act was enacted to deal with surveillance of all electronic communication.

the Vision

THE PEGASUS PROJECT

► Paris-based media nonprofit Forbidden Stories and Amnesty International accessed a leaked database of thousands of phone numbers across the world targeted by a spyware called Pegasus

► They shared the data with global media organisations as part of a collaborative investigation called Pegasus Project

► An Israeli

company called NSO Group makes Pegasus, a spyware capable of extracting data from a phone

According to the report, at least 2 Union Cabinet ministers, 3 opposition leaders, a Constitutional authority, government officials, scientists and over 40 journalists in India were targeted

Key Points

- Telegraph Act:
 - Under Section 5(2) of this law, the government can intercept calls only in certain situations:
 - Interests of the sovereignty and integrity of India,
 - Security of the state,
 - Friendly relations with foreign states or public order,
 - Preventing incitement to the commission of an offence.
 - These are the same restrictions imposed on free speech under Article 19(2) of the Constitution.

- However, these restrictions can be imposed only when there is a **condition precedent** the **occurrence of any public emergency, or in the interest of public safety.**
- Further, the grounds of selecting a person for surveillance and extent of information gathering has to be **recorded in writing.**
- This lawful interception cannot take place against journalists.
 - Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government, unless their transmission has been prohibited under this subsection.
- Supreme Court Intervention: In Public Union for Civil Liberties v Union of India (1996), the SC pointed out lack of procedural safeguards in the provisions of the Telegraph Act and laid down following observations:
 - Tapping is a serious invasion of an individual's privacy.
 - It is no doubt correct that every Government exercises some degree of surveillance operation as a **part of its intelligence** outfit but at the same time **citizen's right to privacy has to be protected.**
- **Sanction for Interception:** The abovementioned Supreme Court's observations formed the basis of **introducing Rule 419A** in the Telegraph Rules in 2007 and later in the rules prescribed under the IT Act in 2009.
 - Rule 419A states that a Secretary to the Government of India (not below the rank of a Joint Secretary) in the Ministry of Home Affairs can pass orders of interception in the case of Centre, and similar provisions exist at the state level.

• IT Act, 2000:

- Section 69 of the Information Technology Act and the Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were enacted to further the legal framework for electronic surveillance.
- However, the scope of Section 69 the IT Act is much broader and vague than the Telegraph Act as the only condition precedent for engaging electronic surveillance is for the "investigation of an offence".
- These provisions are problematic and offer the government total opacity in respect of its interception and monitoring activities.
- Associated Issues with the Surveillance:
 - Legal Loopholes: According to the Centre for Internet & Society, the gaps in laws allow surveillance and affect privacy. For example:
 - Ambiguity on issues like type of interception, granularity of information that can be intercepted and the degree of assistance from service providers helps in bypassing the law and aids surveillance by the state.
 - Affects Fundamental Rights: The very existence of a surveillance system impacts the right to privacy (held by the SC in <u>K.S. Puttaswamy v. Union of India case, 2017</u>) and the exercise of freedom of speech and personal liberty under <u>Articles 19 and 21 of the Constitution.</u>
 - **Authoritarian Regime:** The surveillance promotes spread of authoritarianism in the government functioning since it allows the executive to exercise a disproportionate amount of power on the citizen and impacts their personal lives.
 - **Threat to Freedom of Press:** Current revelations over the use of Pegasus highlights that surveillance was also conducted on many journalists. This affects freedom of press.

Way Forward

- There is a need for reforms in the Indian surveillance regime, which should incorporate ethics of surveillance and considers the moral aspects of how surveillance is employed.
- In this context, there is a need for a holistic debate before the <u>Personal Data Protection (PDP)</u> <u>Bill, 2019</u> is enacted.
- So that the law can be tested against the cornerstone of fundamental rights and growth of

the digital economy and security of the country can be balanced.

Source: IE

PDF Refernece URL: https://www.drishtiias.com/printpdf/surveillance-laws-in-india-and-privacy

