Pegasus Case

What is the issue?

Supreme Court has set up a panel to investigate allegations of potential surveillance of mobile phones using the Pegasus spyware.

What is Pegasus?

> *A spyware is any malicious software designed to enter your computer device, gather your data, and forward it to a third-party without your consent.*

- Pegasus is a spyware developed by an Israeli firm, NSO Group, to infiltrate smartphones — Android and iOS — and turn them into surveillance devices.
- It is used as a tool to track criminals and terrorists for targeted spying and not mass surveillance.
- NSO Group has affirmed that it sells the software only to governments.

How does it work?

- Pegasus exploits undiscovered vulnerabilities or bugs, which means a phone could be infected even if it has the latest security patch installed.
- In 2016 smartphones were infected using a technique called "**spear-fishing**": text messages or emails containing a malicious link were sent to the target and it depended on the target clicking the link.
- By 2019, Pegasus employed **zero-click installation** without requiring any interaction by the target"
- It could infiltrate a device with a missed call on WhatsApp and could even delete the record of this missed call, making it impossible for the user to know they had been targeted.
- Pegasus also exploits bugs in iMessage, giving it backdoor access to millions of iPhones.
- The spyware can also be installed over a wireless transceiver (radio transmitter and receiver) located near a target.

What happened with Pegasus spyware?

- The Pegasus Project, an international investigative journalism effort, revealed that various governments used the software to spy on government officials, opposition politicians, journalists, activists and many others.
- It said the Indian government used it to spy on around 300 people between 2017 and 2019.
- A case was filed in the Supreme Court accusing the government for indiscriminate spying.

What was the government's stand?

- The government refused to file a detailed response to the allegations made by the petitioners citing national security as a reason.
- The government also pled to set up its own probe which was rejected by the court.
- The court said that such a course of action would violate the settled judicial principle against bias, i.e., "justice must not only be done, but also be seen to be done".

What was the court's view?

- The Supreme court has underlined three key imperatives
    1. The right to privacy of citizens
    2. Freedom of the press including the right of journalists to ensure protection of their sources
    3. Limits on the usage of national security as a shield by the government to block disclosure of facts related to citizen's rights.
- The court cited the ***Ram Jethmalani v. Union of India 2011*** to say that the Government should not take an adversarial position when the fundamental rights of citizens are at threat.
- The court said that the Union of India may decline to provide information citing security of the State or other specific immunity under a specific statute but they must prove and justify the same.
- It has set seven terms of reference for the committee such as who procured Pegasus and whether the petitioners in the case were indeed targeted by use of the software, etc.

- The court has also asked the committee to make recommendations on a legal and policy framework on cyber security to ensure the right to privacy of citizens is protected.

What were the earlier views regarding privacy?

The right to privacy is protected as an intrinsic part of the right to life and personal liberty under ***Article 21***

The expression "freedom of press" has not been issues in Article 19 but it is comprehended within ***Article 19(1)(a)***

- The ***2017 K.S. Puttaswamy judgment*** clarified that any invasion of privacy could only be justified if it satisfied three tests:
  1. The restriction must be by law
  2. It must be necessary (only if other means are not available) and proportionate (only as much as needed)
  3. It must promote a legitimate state interest (e.g., national security)]
- In 2018, the **Srikrishna Committee** on data protection noted that post the K.S. Puttaswamy judgment, most of India's intelligence agencies are "potentially unconstitutional" because they are not constituted under a statute passed by Parliament.

References

1. https://www.thehindu.com/todays-paper/tp-opinion/a-credible-probe/article37203576.ece
2. https://indianexpress.com/article/explained/why-was-pegasus-panel-needed-what-it-will-do-now-and-how-7594273/
3. https://indianexpress.com/article/explained/pegasus-snoop-allegations-sc-moved-the-needle-on-privacy-press-freedom-govt-security-alibi-7594235/
4. https://economictimes.indiatimes.com/tech/trendspotting/what-is-pegasus-spyware-and-how-it-works/articleshow/84607533.cms?from=mdr



SHANKAR
IAS PARLIAMENT
Information is Empowering