MHA Notification on Computer Surveillance – III

Click here to know more on the issue

\n\n

What law covers tapping phones/computers?

\n\n

\n
- Lawful interception of phones and computers can be done by the governments at the Centre and in the states under Section 5(2) of the Indian Telegraph Act, 1885.
\n
- If it is done illegally, it is punishable under sections 25 & 26 that provide for imprisonment up to three years, with or without a fine.
\n

\n\n

When is tapping by the government lawful or illegal?

\n\n

\n
- The Supreme Court laid down the following guidelines in this regard in the **PUCL vs Union of India** case.
\n
- Section 5(2) of ITA,1985 does not confer unguided and unbridled power on investigating agencies to invade a person's privacy.
\n
- Tapping of telephones is prohibited without an authorising order from the Home Secretary of the Union government or of the state government concerned.
\n
- The order unless is valid for two months and if renewed, it cannot remain in operation beyond six months.
\n
- Phone tapping or interception of communications must be limited to the address specified in the order or to addresses likely to be used by a person specified in the order.
\n

- All copies of the intercepted material must be destroyed as soon as their retention is not necessary under Section 5(2).
\n

\n\n

Who oversees if interception is done without misuse of powers?

\n\n

\n
- There is no judicial or parliamentary oversight to review cases of lawful interception.
\n
- However, the orders of the competent authority clearing lawful interception are reviewed by a review committee at both the central and state levels under Rule 419-A of the Indian Telegraph Rules, 1951.
\n
- The review committee investigates whether its passing is relevant within two months of an order.
\n
- Rule 419-A also provides for the procedure and precautions for handling lawful interception cases to ensure that unauthorised interception does not take place.
\n

\n\n

What are the rules for monitoring of emails and social media content?

\n\n

\n
- This is done by invoking the provisions of “public emergency”, “interest of sovereignty” or “integrity of India”.
\n
- Under Section 69 of the IT Act, 2008, the central and state governments are empowered to issue directions to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resources.
\n
- Accordingly, the Ministry of Home Affairs in 2011 issued standard operating procedures (SOPs) to law enforcement agencies.
\n
- The Department of Telecom has also issued SOPs for lawful interception to the telecom service providers.
\n

\n\n

What does the SOP contain?

\n\n

\n
- It requires setting up of an internal evaluation cell that will examine a monthly statement from law-enforcement agencies on the fifth of succeeding month.
\n
- These statements are to detail the authorisation orders received for interception, numbers and emails intercepted including period of interception, number of telephones and emails authorised but not intercepted, etc.
\n
- The SoPs also mention the need for destruction of data and phone-tapping records beyond six months.
\n
- It further says that for surveillance in remote areas, the competent authority should be informed within 3 days and permission must be obtained in 7 days, failing which the interception will not be valid.
\n

\n\n

\n\n

Source: The Indian Express

\n