MHA Notification on Computer Surveillance

Why in news?

\n\n

Ministry of Home Affairs (MHA) recently issued a notification authorising 10 central agencies to intercept information related to computer resource.

\n\n

What does the notification say?

\n\n

\n
- The government authorised 10 central agencies to intercept, monitor and decrypt any information generated, transmitted, received or stored in any computer in the country.
\n
- These agencies include Intelligence Bureau, Narcotics Control Bureau, Enforcement Directorate, Central Board of Direct Taxes, Directorate of Revenue Intelligence, CBI, NIA, Cabinet Secretariat (RAW), Directorate of Signal Intelligence and the Commissioner of Police, Delhi.
\n
- The order is facilitated under sub-section 1 of the section 69 of the IT Act, read with rule 4 of the Information Technology Rules, 2009.
\n
- The IT Act allows the authorities to decrypt information if it is in the interest of –
\n

\n\n

\n
1. The sovereignty or integrity of India
\n
2. The security of the State
\n
3. Friendly relations with foreign States
\n
4. Public order
\n

5. Preventing incitement to the commission of any cognisable offence.
\n

\n\n

\n

- The IT rules states that a competent authority can authorise a government agency to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource.
\n
- However, opposition leaders and experts have called it “unconstitutional” and “an assault on fundamental rights”.
\n

\n\n

What is the clarification given by the Home Ministry?

\n\n

\n

- The notification is aimed at ensuring that any interception, monitoring or decryption of any information through any computer resource is done in accordance with due process of law.
\n
- It is also aimed at preventing any unauthorized use of these powers by any agency, individual or intermediary.
\n
- All agencies will have to take the approval of the Home Secretary before intercepting or monitoring data stored in computer.
\n
- These powers are also available to the competent authority in the State governments as per IT Rules 2009.
\n
- The order is in accordance with rules already framed in 2009 and hence no new power has been conferred to any of the security or law enforcement agencies.
\n
- Also, similar provisions and procedures already exist in the Telegraph Act along with identical safeguards.
\n
- The present notification is analogous to the authorisation issued under the Telegraph Act.
\n

\n\n

What are the concerns?

\n\n

\n
- Content streams are getting much richer, pervasive and personal.
\n
- Hence the order is unconstitutional and in breach of the telephone tapping guidelines, the (Right to) Privacy judgment and the Aadhaar judgment.
\n
- **Provisions** - Phrasing of "intercept" in the rules might include traffic diversion, which may permit code injections and malware attacks.
\n
- The notification also permits decryption, which might require the service provider to break their encryption protocols.
\n
- **Clearance** - The home ministry says that each case will continue to be approved by the Union home secretary.
\n
- But a specific clearance on each case is obviously meaningless because the record shows about 100 clearances daily on average.
\n
- The scrutiny is therefore remains only on paper, and there is no safeguard against misuse.
\n
- Also, the rules provided that the home secretary's clearance should be obtained within a week.
\n
- This could make the agencies to tap at will without clearance.
\n
- **Safeguards** - There is a blanket authorisation being given to security agencies, without any safeguards regarding its misuse.
\n
- This was given even to foreign-focused agencies that have no business on surveillance of Indian citizens such as the Research & Analysis Wing.
\n
- **Control** - Many of the agencies named in the order from the home ministry are neither under parliamentary scrutiny nor are their actions subject to judicial control.
\n

\n\n

What should be done?

\n\n

\n
- The courts have made the home secretary accountable for all surveillance by

central agencies and created a monitoring committee in 1996.
\n
- Since then, the occasions for digital surveillance have grown manifold.
\n
- The only way to deal with a lack of capacity for due process is to increase the capacity available, and not to subvert the due process.
\n
- Reason should be given before taking up any case and responsibilities should be assigned for the surveillance agencies.
\n
- Such cases also need authorisation from a magistrate, who has to record the specific reasons in each case.
\n
- Any well-constructed system of surveillance should balance both public security and individual rights.
\n
- Thus, this should be considered an opportune moment to reform India's intelligence apparatus and bring it on a sound legal and constitutional footing.
\n

\n\n

\n\n

Source: Business Standard

\n