Science & Technology · GS - III

Can mandatory SIM verification of messaging applications effectively address cybercrime without compromising digital privacy? Discuss.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 23/10/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
10	~150 words

Answer Hint

Cybercrime prevention, digital identity, SIM verification, user accountability, privacy, data protection, digital inclusion, proportional regulation, cybersecurity.

Model Answer

Introduction:

Digital messaging platforms have become important channels for communication but can also be misused for fraud, impersonation and other cybercrimes. SIM verification is one possible regulatory response.

Potential Benefits

1. Traceability: Verified mobile numbers can provide useful leads during investigations.
2. Accountability: Linking accounts to verified numbers may discourage certain forms of misuse.
3. Law enforcement: Properly regulated information-sharing can support investigations into cyber fraud.

•

Concerns and Limitations

1. Privacy: Excessive collection or sharing of user data may expose personal information.
2. Limited effectiveness: Fraudsters can use stolen SIMs, compromised accounts or other identities.

3. Digital exclusion: Strict requirements may inconvenience legitimate users who change numbers or lack reliable mobile access.

Way Forward:

Regulations should establish clear legal safeguards, data minimisation, secure verification systems, independent oversight and accessible grievance mechanisms. They should complement, rather than replace, cybercrime investigation and public awareness.

Conclusion:

SIM verification may strengthen accountability, but effective cybercrime prevention requires a balanced framework that protects both national security and citizens' digital rights.

BECOME IAS
AI POWERED UPSC PREP