Defence & Security · GS - III

Data security has assumed significant importance in the digitized world due to rising cyber-crimes. The Justice B. N. Srikrishna Committee Report addresses issues related to data security. What, in your view, are the strengths and weaknesses of the Report relating to protection of personal data in cyber space?

EXAM YEAR	PAPER	SUBJECT
2018	GS - III	Defence & Security

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Personal data protection; consent and purpose limitation; individual rights; data fiduciaries; Data Protection Authority; state exemptions; compliance costs; digital privacy

Model Answer

Introduction

The Justice B. N. Srikrishna Committee submitted its report on data protection in 2018, along with a draft Personal Data Protection Bill. It sought to create a legal framework for privacy and responsible processing of personal data.

Strengths of the Report

1. **Privacy protection:** It recognised informational privacy as a core concern in the digital economy.
2. **Consent and purpose limitation:** Personal data should be collected and processed for specified purposes under defined conditions.
3. **Individual rights:** The proposed framework provided rights concerning access, correction and control over personal information.

4. **Accountability:** Data fiduciaries were expected to adopt safeguards, security practices and compliance procedures.
5. **Institutional oversight:** A proposed Data Protection Authority would supervise compliance and address violations.
6. **Cross-border regulation:** It addressed the transfer and handling of personal data outside India.

Weaknesses and Concerns

1. **State exemptions:** Broad exemptions for government processing raised concerns about surveillance and insufficient safeguards.
2. **Data localisation:** Certain localisation requirements could increase compliance costs and complicate cross-border digital services.
3. **Implementation burden:** Smaller firms and startups might struggle with complex compliance obligations.
4. **Regulatory independence:** Effective protection requires an authority capable of acting independently and transparently.
5. **Balancing interests:** Overly restrictive rules could hinder research, innovation and legitimate data use if safeguards are poorly designed.

Way Forward

A sound framework should provide narrowly defined exemptions, independent oversight, effective remedies, strong cybersecurity standards and proportionate compliance requirements. Transparency and public consultation are essential.

Conclusion

The Committee's report established an important foundation for personal-data protection, but its effectiveness depends on balancing privacy, state accountability, innovation and practical enforcement.