



## Need for New IT Law

**For Prelims:** Information Technology Act, 2000, Cybercrimes, Splinternet, Section 66A of the IT Act, Data Protection law

**For Mains:** Need for Review of Information Technology Act, 2000, Cyber Security, IT & Computers, Government Policies & Interventions

### Why in News?

Recently, the **Minister of State for Electronics and Information Technology (IT)** spoke on the need for legislative overhaul of the **22-year-old Information Technology Act, 2000**.

- The government enacted the [original IT legislation in 2000](#).
- The **IT (Amendment) Act came into force in 2009** and was aimed at facilitating [e-governance](#), [preventing cybercrime](#) and [fostering security practices](#) within the country.
- Recently, the government has notified [Information Technology \(Intermediary Guidelines and Digital Media Ethics Code\) Rules 2021](#).

### Why is there a need for New IT Law (External Issues)?

- **India Entering into Digital Age:** India is going to have a [trillion-dollar digital economy](#) in a few years, and a large number of businesses will be on the Indian Internet.
  - Therefore, an **open & secure Internet** becomes an important economic component of our country.
- **Rise of Splinternet:** The global internet as we know it is on the verge of **splintering into smaller bubbles of national networks** due to aggressive national policies, trade disputes, censorship, and dissatisfaction with **big tech companies**.
  - This will have far-reaching consequences that impact international unions, data enterprises and individual consumers alike.
  - Perhaps the most sophisticated instance of a splintered internet today would be **China's Great Firewall**.
  - What are seen as essential services, like **Google Search and Maps, Western social media**, and so on – are **entirely banned and replaced by Chinese alternatives like Weibo** in the name of Cyber Sovereignty

### Why is there a need for New IT Law (Internal Issues)?

- **Majority of Cybercrimes in India are Bailable Offense:** A historical mistake was made when the **IT (Amendment) Act, 2008**, made almost all cybercrimes, barring a couple, bailable offences.
  - The focus was more on enhancing the **quantum of civil liability** and reducing the quantum of punishment, which explains the reason why the number of cybercrime convictions in the country is in single digits.
- **Restricted Cyber Security Remedy:** IT Act is effective in metropolitan cities like Mumbai, Delhi,

Hyderabad, Bhopal, Bangalore, etc., but it is **feeble in tier-two level cities as awareness of the law** by enforcement agencies remains a big challenge.

- The IT Act **does not cover most crimes committed through mobiles**. This needs to be rectified.

## What are Present Government Initiatives for Cyber Security?

- [Cyber Surakshit Bharat Initiative.](#)
- [Cyber Swachhta Kendra.](#)
- [Online cybercrime reporting portal.](#)
- [Indian Cyber Crime Coordination Centre \(I4C\).](#)
- [National Critical Information Infrastructure Protection Centre \(NCIIPC\).](#)
- [Information Technology Act, 2000.](#)

## Way Forward

- The government is looking at a **new legislative framework** with the new rulemaking capabilities that deal with various issues related to digital space. This **should include**:
  - The majority of cybercrimes need to be made **non-bailable offences**.
  - A comprehensive **data protection regime** needs to be incorporated in the law to make it more effective.
  - **Cyber war** as an offence needs to be covered under the IT Act.
  - Parts of **Section 66A of the IT Act** are beyond the reasonable restrictions on freedom of speech and expression under the Constitution of India. These need to be removed to make the provisions legally sustainable.
- Increasingly **bilateral or multilateral arrangements between countries will have to evolve** in such a way that nothing can be done in isolation from other countries.

## UPSC Civil Services Examination, Previous Year Questions (PYQs)

**Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)**

1. Service providers
2. Data centres
3. Body corporate

**Select the correct answer using the code given below:**

- (a) 1 only  
(b) 1 and 2 only  
(c) 3 only  
(d) 1, 2 and 3

**Ans: (d)**

**Explanation:**

- According to section 70B of the Information Technology Act, 2000 (IT Act), the Union Government by notification should appoint an agency named **Indian Computer Emergency Response Team (CERTIn)** to serve as the national agency for incident response.

**Source: TH**

PDF Refernece URL: <https://www.drishtias.com/printpdf/need-for-new-it-law>

