



## Convention on Global Cybercrime

---

 [drishtiias.com/printpdf/convention-on-global-cybercrime](https://drishtiias.com/printpdf/convention-on-global-cybercrime)

### Why in News

---

India voted in favour of a cybercrime resolution led by Russia in a committee of the United Nations General Assembly. The resolution seeks to set up new cyber norms considered as counter alternative to the US backed Budapest Accord.

A final General Assembly vote to adopt the resolution will be held in December, 2019.

### Budapest Convention

---

- The **Council of Europe's (CoE) Cybercrime Convention** is also known as the Budapest Convention. It was open for signature in 2001 and came into force in 2004.
- The convention is the **sole legally binding** international multilateral treaty on cybercrime. It **coordinates cybercrime investigations** between nation-states and **criminalizes** certain cybercrime conduct.
- It serves as a **guideline for any country developing comprehensive national legislation against Cybercrime** and as a **framework** for international cooperation between state parties to this treaty.

The Budapest Convention is supplemented by a **Protocol on Xenophobia and Racism** committed through computer systems.

- **Significance:** Almost all stakeholders agree that the current form of cross-border data sharing for law enforcement through the **Mutual Legal Assistance Treaty (MLAT)** is insufficient for the digital age. However, there is an ongoing debate whether to revamp MLAT or form an entirely new system for cybercrimes in the form of this Convention.
- This Convention has eagerly called for Indian participation since its formation in 2001, but **India has decided not to be a party to it.**

### Russia-led Resolution

---

- The Russian proposal entitled ***“Countering the use of information and communications technologies for criminal purposes”*** was recently put forth in the **United Nations General Assembly (UNGA)**.

This recent UN proposal follows previous Russian initiatives, including the “Draft United Nations Convention on Cooperation in Combating Cybercrime” in 2017 to develop a UN convention on cybercrime.

- The Russian proposal calls for creation of a committee that will convene in August 2020 in New York in order to **establish a new treaty through which nation-states can coordinate and share data to prevent cybercrime.**
  - This draft Convention goes far beyond what the Budapest Convention allows for regarding cross-border access to data, including limiting the ability of a signatory to refuse **to provide access to requested data.**
  - This is the reason why several human rights groups criticize the UN proposal as a way to extend a Chinese and Russian form of internet governance, or the so-called “closed Internet” or “state-controlled internet.”
- If this resolution will be passed by the UNGA, it will become the second international convention on cybercrime.
- Russia and China question the Budapest Convention on the grounds of national sovereignty issues, thereby proposing their own treaty at the UN.

## India’s Stand

---

- India maintained its status as a non-member of the Europe-led Budapest Convention. Although, India voted in favour of a Russian-led UN resolution to set up a separate convention.
- According to the **Intelligence Bureau (IB)**, data sharing with foreign law enforcement agencies infringes on national sovereignty of India.
- India has also previously argued that it will not sign onto the Budapest treaty since it was drafted **without its participation.**

## Data Laws in India

---

Data protection laws in India are currently facing many problems and resentments due to the absence of a proper legislative framework. The legal framework includes:

- **Information Technology Act, 2000:** IT Act contains provisions (For example, mentioned in section 43A, 72A) regarding cyber and IT-related laws in India.
  - **Section 43A:** Compensation for failure to protect data.
  - **Section 72A:** Any disclosure of information, knowingly and intentionally, **without the consent** of the person concerned has been made punishable with imprisonment for a term extending to three years.
- However, these provisions neither protect any breach of information on the one hand nor enforce a right-based framework on privacy.

Supreme Court in ***Justice K. S. Puttaswamy (Retd.) Vs Union of India*** (2017) unanimously held that citizens have a constitutionally protected **fundamental right to privacy** that forms **an intrinsic part of life and liberty under Article 21.**
- Therefore, in order to establish a strong data protection regime, the government has proposed the **Draft Personal Data Protection Bill, 2018** (based on the recommendation of Justice BN Srikrishna Committee).

**Source: IE**