India's Tech Regulatory Landscape

This editorial is based on "Big Tech's excesses" which was published in The Hindu Business Line on 22/11/2024. The article brings into picture the CCI's landmark penalty on Meta, emphasizing the intersection of privacy and competition law while highlighting India's need for a comprehensive data protection framework to address vulnerabilities in user rights.

For Prelims: Competition Commission of India, EU's General Data Protection Regulation, Information Technology Act, 2000, IT Rules, 2021, RBI's Data Localization Norms, Consumer Protection Act, 2019, E-commerce Rules, 2020, Economic Survey 2023-24.

For Mains: Current State of Technology Regulation in India, Key Challenges in India's Technological Landscape

Competition Commission of India's recent penalty on Meta marks a watershed moment in **tech regulation,** spotlighting the intersection of privacy and competition law. The CCI's decision, triggered by **WhatsApp's controversial 2021 Privacy Policy,** challenges the coercive data-sharing practices of tech giants and their **abuse of market dominance.** Unlike the **EU's General Data Protection Regulation**, which prevented WhatsApp from implementing similar policies in Europe, India's **delayed implementation of Personal Data Protection Law** leaves users vulnerable to data exploitation.

What is the Current State of Technology Regulation in India?

- **Competition Law Framework**
  - **Competition Act, 2002**: Empowers the **Competition Commission of India (CCI)** to investigate and regulate anti-competitive practices, including those in digital markets.
    - **Key Amendments (2023)**: Deal value thresholds added to **address high-value acquisitions.**
  - **Notable Enforcements**: Actions against major tech companies like **Google and Meta** for abuse of market dominance.
- **Digital Infrastructure Regulations**
  - **Information Technology Act, 2000**: Serves as the primary legislation for governing **digital transactions, cybersecurity, and cybercrime.**
  - **IT Rules, 2021**: Comprehensive regulations targeting social media platforms, OTT services, and digital news media:
    - Mandates robust **grievance redressal mechanisms**.
    - Imposes obligations for **content moderation**, **takedowns**, and **user verification**.
- **Data Protection Framework**
  - Operates under **Section 43A** of the **IT Act** and **Digital Personal Data Protection Act 2023.**
- **Sector-Specific Regulations**

    - **Banking and Finance**:: RBI guidelines for fintech companies and digital payment platforms.
        - **RBI's Data Localization Norms** mandate local storage for payment data.
    - **Telecom and OTT**: **TRAI** regulations for over-the-top communication services.
        - It also sets telecom norms for digital infrastructure and internet services.
    - **Financial Markets**: **SEBI** guidelines for automated trading.
- **Consumer Protection Mechanisms**
    - **Consumer Protection Act, 2019**: Incorporates dedicated e-commerce guidelines.
    - **E-commerce Rules, 2020**: Focuses on **addressing unfair trade practices, fraudulent activities, and consumer rights** violations in digital marketplaces.
- **Proposed Legislation and Policies**
    - **Digital India Act**: Expected to replace the IT Act, 2000.
    - **National Data Governance Framework** (Draft): Focuses on data sovereignty and digital governance.

What are the Key Challenges in India's Technological Landscape?

- **Digital Divide and Infrastructure Gap:** India's digital transformation is severely hampered by the **urban-rural infrastructure disparity**, with rural areas lacking both quality connectivity and digital literacy.
    - The divide particularly affects marginalized communities**, creating a two-tier digital citizenship** that threatens inclusive growth.
    - According to **TRAI's October 2024 report,** while **urban teledensity** stands at **132.94%**, **rural teledensity** remains at just **59.05%**, highlighting the stark divide.
- **Fragmented Regulations**:India's technology sector faces regulatory inefficiencies due to overlapping jurisdictions of multiple agencies, leading to compliance confusion for businesses.
    - For instance**, data protection, digital content, and cyber laws** are governed by different authorities without a unified framework
    - This fragmented approac**h increases operational complexity and slows innovation.**
    - Additionally, businesses operating globally face challenges in reconciling India's data localization mandates with international standards like the **EU's GDPR, creating barriers to seamless data flow and interoperability.**
- **Data Privacy and Security Vulnerabilities:** The lack of implementation of **Digital Personal Data Protection Act 2023** has left Indian citizens **vulnerable to data breaches and privacy violations,** particularly affecting sensitive sectors like healthcare and finance.
    - Tech companies continue to exploit this **regulatory vacuum by implementing invasive data collection practices** without adequate safeguards.
    - CERT-In reported **13.91 Lakh cyberattack incidents in 2022**, highlighting the gravity of the issue.
- **Platform Monopolies and Market Distortion:** Big tech companies' dominance in Indian digital markets has **created insurmountable entry barriers for local competitors**, stifling innovation and consumer choice.
    - These monopolistic practices **extend beyond market dominance to data control and ecosystem lock-ins**.
    - The concentration of power allows these platforms to dictate terms to both businesses and consumers.
    - The CCI has imposed a **five-year ban on WhatsApp sharing data with Meta** and fined **Rs 213.14 crore for antitrust violations in India**, exemplifying the growing concern over market concentration.
- **AI Governance and Ethics:** India's rapid adoption of **AI technologies without corresponding ethical frameworks** and regulatory oversight creates risks of algorithmic bias and privacy violations.
    - The **absence of standardized testing and certification processes** for AI systems leaves citizens vulnerable to automated decision-making biases.
    - India currently lacks specific laws directly **addressing generative AI, deepfakes, and AI-related crimes that are on the rise.**
    - Two individuals in Bengaluru, India, were recently scammed out of **nearly Rs 1 crore** by fraudsters using deepfake videos of business leaders **N. R. Narayana Murthy and Mukesh Ambani.**

        - The **victims were lured into investing in fake trading platforms** promoted through these manipulated videos, highlighting the growing threat of deepfakes in financial fraud.
- **Digital Skills Mismatch**: The technology sector faces a critical talent crisis as **traditional education fails to keep pace with rapidly evolving industry needs**.
    - The skills gap particularly affects emerging technologies, creating a bottleneck in India's digital transformation journey.
    - The mismatch between education and industry requirements leads to both unemployment and unfilled positions.
    - Only **51.25% of India's graduates are employable**, with significant challenges in vocational training and skilling, according to the **Economic Survey 2023-24.**
- **Cross-Border Data Flow Restrictions** India's data localization requirements, while **aimed at sovereignty**, create operational inefficiencies and increased costs for global digital services.
    - The restrictions **impact India's position in the global digital economy** and affect service quality for Indian users.
    - The compliance burden particularly affects smaller companies and startups looking to operate globally.
    - Fintech firms usually spend around **6-10% of their operating costs on compliance.**
- **Content Regulation Balance:** The increasing **government control over digital content through takedown requests** and platform regulations threatens free expression and innovation in the digital space.
    - The **ambiguity in content moderation guidelines** creates uncertainty for platforms and content creators.
    - The regulatory framework often prioritizes control over fostering a vibrant digital ecosystem.
    - The Indian government submitted **63,852 requests for user data to social media giant Meta in the second half of 2022** (from July to December), second only to the US.
    - Also, recently the Supreme Court has halted the implementation of the **Fact-checking Unit (FCU) Rules** issued by the Union Government until the Bombay High Court decides on challenges to the **IT Rules amendment 2023,** citing serious **constitutional concerns affecting freedom of speech.**

What Lessons can India Learn from Other Countries in Terms of Technological Regulation?

- **European Union (EU):** The EU has established significant global influence through its regulatory frameworks, such as the **General Data Protection Regulation (GDPR).**
    - These regulations have not only affected EU-based companies but have had a global impact, with many international firms adopting EU standards in their operations, a phenomenon known as the **"Brussels Effect."**
- **Australia - News Media Bargaining Code:** Australia's innovative approach to platform-media relationships forced tech giants to negotiate fair compensation with news organizations.
- **South Korea - Platform Regulation** Korea's pioneering app store regulation **(first to mandate alternative payment systems)** and strong data protection framework offers valuable lessons.
- **Estonia - Digital Government**: Estonia's comprehensive e-governance framework, **with 99% of public services online**, showcases effective digital transformation.
- **Japan - Digital Platform Transparency**: **Japan's Transparency Act** focuses on fair business practices and disclosure requirements for major digital platforms.

What Steps can be Taken to Enhance India's Technological Regulatory Framework?

- **Unified Digital Regulatory Authority:** The creation of a **centralized regulatory body** would streamline the currently fragmented oversight of digital services and technology platforms.
    - This authority should integrate expertise from **CCI, TRAI, CERT-In, and other relevant**

bodies to provide cohesive regulation across digital domains.
    - The UDRA could establish a **single-window clearance system for tech companies,** reducing compliance burden while ensuring comprehensive oversight building upon **Justice B.N. Srikrishna Committee's recommendations.**
    - The authority should be **granted autonomous status similar to RBI,** with technical experts leading specialized divisions for **AI, data protection, platform governance, and cybersecurity.**
- **Tiered Compliance Framework:** Implementing a size-based regulatory approach where **obligations increase with platform scale and market impact would balance innovation with oversight**.
    - Start-ups and small platforms would face minimal compliance requirements, while significant platforms would have enhanced responsibilities including mandatory audits and transparency reports.
    - This framework should include **clear thresholds based on user base, revenue, and market impact**, with specific compliance requirements at each tier.
- **Mandatory Interoperability Standards:** Developing and enforcing **interoperability standards for digital platforms** would reduce monopolistic control and enhance competition.
    - Key services like **messaging, social media, and digital payments should be required to support data portability** and cross-platform functionality.
    - The standards should be developed through multi-stakeholder consultation, with clear implementation timelines and technical specifications. This would include **mandatory APIs for data exchange and common protocols** for cross-platform communication.
- **Regional Digital Innovation Zones:** Establishing specialized technology zones across **tier-2 and tier-3 cities with simplified regulations** and infrastructure support to make decentralized innovation zones tied to **District Development Plans** ensuring equitable digital growth.
    - These zones should offer **tax incentives, high-speed connectivity, and regulatory sandboxes for testing new technologies** and business models.
    - The zones could focus on specific technological domains like AI, IoT, or blockchain, creating specialized ecosystems across regions. **Local universities should be integrated into these zones** to bridge the industry-academia gap.
- **Digital Literacy and Skill Development Framework:** Creating a **nationwide digital skills program** with standardized certification and industry recognition would address the technology talent gap.
    - The framework should **combine online learning platforms with hands-on training centers in partnership** with industry leaders.
    - Mandatory **digital literacy modules should be integrated into school curricula** and adult education programs.
    - Special focus should be given to **emerging technologies and regular curriculum updates based on industry needs.** The framework should include targeted programs for rural areas and underserved communities.
- **Data Protection Implementation Task Force:** Establishing a **dedicated task force to oversee the implementation of data protection regulations** would ensure effective enforcement and compliance support.
    - The task force should include **technical experts, legal professionals, and industry representatives** to provide practical implementation guidelines.
    - Regular audits and compliance reports should be mandated for organizations handling significant amounts of personal data.
    - The task force should also facilitate training programs for **Data Protection Officers and maintain a public registry of certified professionals**.
    - Launched in 2020 by the Ministry of Finance and RBI**, Data Empowerment and Protection Architecture (DEPA)** enables secure, consent-based data sharing through **third-party Consent Managers** enhancing data governance, and can serve as a model.
- **AI Governance Framework:** Developing a comprehensive AI governance structure with **clear guidelines for development, testing, and deployment of AI systems is crucial.**
    - The framework should establish **mandatory impact assessments for high-risk AI applications** and certification requirements for AI systems used in critical sectors.
    - Regular audits of AI systems for bias and fairness should be mandated, with public reporting of results. The framework should include **clear liability provisions for AI-**

related incidents and mandatory insurance requirements for high-risk applications.

- **International Collaboration to Harmonize Cross-border Data Flow:** Establishing **clear protocols for international data transfers** while protecting national security interests would facilitate global digital trade.
    - The protocol should include **standardized data classification systems and specific requirements** for different data categories.
    - Bilateral and multilateral agreements should be pursued for **mutual recognition of data protection standards.** The protocol should include emergency mechanisms for addressing cross-border data breaches and disputes.
- **Platform Competition Enhancement:** Implementing measures to **promote competition in digital markets** through mandatory app store alternatives and payment system choices like the **Unified Payments Interface (UPI)**, that has revolutionized digital payments in India by **fostering interoperability and reducing entry barrier**s for fintech companies.
    - Clear guidelines for **platform pricing and revenue sharing should be established to protect small businesses**.
    - The measures should include **mandatory disclosure of ranking algorithms and clear appeal mechanisms** for business users.

Conclusion:

India's tech landscape, while brimming with potential, faces significant regulatory challenges. A **comprehensive and adaptive regulatory framework** is crucial to balance innovation with consumer protection and national security interests. By learning from **global best practices and addressing the specific needs of the Indian context,** India can create a robust digital ecosystem that empowers citizens, fosters innovation, and drives economic growth.

Drishi Mains Question:

What are the key challenges in India’s technological regulation, and how can global models like the EU’s General Data Protection Regulation influence India’s regulatory framework?

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Prelims

Q1. ‘Right to Privacy’ is protected under which Article of the Constitution of India? (2021)

(a) Article 15

(b) Article 19

(c) Article 21

(d) Article 29

Ans: (c)

Q2. Right to Privacy is protected as an intrinsic part of Right to Life and Personal Liberty. Which of the following in the Constitution of India correctly and appropriately imply the above statement? (2018)

(a) Article 14 and the provisions under the 42nd Amendment to the Constitution.

(b) Article 17 and the Directive Principles of State Policy in Part IV.

(c) Article 21 and the freedoms guaranteed in Part III.

(d) Article 24 and the provisions under the 44th Amendment to the Constitution.

Ans: (c)

Q3. With reference to 'consumers' rights/privileges under the provisions of law in India, which of the following statements is/are correct? (2012)

1. Consumers are empowered to take samples for food testing.
2. When a consumer files a complaint in any consumer forum, no fee is required to be paid.
3. In case of death of consumer, his/her legal heir can file a complaint in the consumer forum on his/her behalf.

Select the correct answer using the codes given below:

(a) 1 only

(b) 2 and 3 only

(c) 1 and 3 only

(d) 1, 2 and 3

Ans: (c)

Mains

Q. Examine the scope of Fundamental Rights in the light of the latest judgement of the Supreme Court on Right to Privacy. (2017)
