

DeepStrat Tech Policy Roundup



DEEPSTRAT

STRATEGY . POLICY . ACTION

2023

Overview

2023 was an eventful year in India's tech policy landscape and for us at DeepStrat. We expanded our policy risks vertical, engaged in several public consultations, undertook new projects, published several studies, built collaborations, and designed solutions. This is a recap of how the landscape evolved and the key issues we worked on.

India's first privacy law, the Digital Personal Data Protection (DPDP) Act, was enacted to safeguard citizen's fundamental right to privacy in the digital space. A new Telecommunications Act was implemented to replace and consolidate pre-colonial telecom regulations. The Information Technology Rules were amended to provision for new forms of intermediary regulation. We worked closely on these key policy developments.

The Ministry of Electronics and Information Technology (MeitY) undertook the mammoth task of replacing over two decades old Information Technology Act of 2000 with the Digital India Act (DIA), to safeguard online safety and trust of Indian internet users. It will act as an overarching framework to regulate the new digital India. We engaged in consultations with the Ministry and published several studies on the proposed themes under the DIA.

As the digital Indian economy grew, so did its threat landscape, resulting in a spike in cyberattacks. The health sector faced two massive cyberattacks this year, which resulted in a major data breach of citizen's Covid test data and technical shutdown of India's premier health institute for several days. Health is a Critical Information Infrastructure (CII) under the IT Act, 2000. Telecom, another CII sector, was at the receiving end of cyberattacks, with the latest being on state-owned telecom operator, BSNL. At DeepStrat, we expanded our cybersecurity offerings, undertook several new projects, published a study on Cloud for CII, and organised training workshops.

The country also witnessed a spike in cybercrimes, an area where offenders are becoming more organised and constantly evolving their techniques, tactics, and procedures. This year DeepStrat helped build a collaborative framework for tackling this key issue, amongst others.

It was also a year that saw significant policy debates and outcomes on regulation of Artificial Intelligence across the globe. It was a momentous year for India as it chaired the Global Partnership on Artificial Intelligence (GPAI), a collaboration that focuses on responsible development and deployment of AI. DeepStrat's paper was selected for GPAI's research symposium and we presented our findings at the GPAI Summit.



Information Technology (Amendment) Rules, 2023

2023 took off with amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The amended Rules brought about new provisions for intermediary regulation. DeepStrat engaged in consultations on the Rules and submitted its recommendations to the Ministry. We highlighted several issues, and studied them closely throughout the year.

First, the business of online gaming (games of skill) was allocated to MeitY, and the first set of regulations for the industry came through this amendment to IT Rules. The Rules defined online gaming and brought about provisions for their regulation, including a self-regulatory framework for the industry. Online gaming is a sunrise sector which has catalysed the growth of digital India and contributed to the creation of indigenous technologies.

Second, the IT Rules brought about provisions to check the spread of misinformation and disinformation through online intermediaries. They brought about a provision for creation of a government controlled fact-check unit. This was challenged in various courts for being violative of fundamental rights and Supreme Court's Shreya Singhal judgment.

The emergence of AI brought about new challenges. AI powered content, such as deepfakes, is not only believable but also indistinguishable from human-generated content. AI has reduced cost and increased the scalability of mis/disinformation. This is a challenge that could have major implications in the upcoming elections. Currently, all these issues are regulated under the two-decades old IT Act, 2000 and the IT Rules, 2023 which are under challenge in several courts.



The Digital Personal Data Protection Act, 2023

Many years in the making, the Digital Personal Data Protection Act was enacted to protect citizen's digital personal data. The law establishes a rights framework flowing from the principles of necessity, legality and proportionality laid down by the Supreme Court in its Puttaswamy-I ruling. Companies or the government can process personal data based on user's consent or a legitimate purpose listed in the Act. Failure to do so, or infringement of user's rights can result in hefty penalties for each breach. The law lays down a three-tiered grievance redressal mechanism – the data fiduciary/consent manager, Data Protection Board and TDSAT.

Many operational details have been left to the Rules, which are expected to be released for consultation soon. The Rules will establish notice requirements, consent manager framework, reporting mechanism for data breaches, timelines, and composition and functions of the Data Protection Board.

Companies have short timelines to comply as the law gets implemented. Compliance will include adopting a consent framework, appointing Data Protection Officers, conducting Data Protection Impact Assessments and periodic audits. As companies step into the role of data fiduciaries, they will have to carefully design measures to inform and protect Indian internet users.

Click [here](#) to read our submission on the DPDP Bill to MeitY last year. Our analysis of the DPDP Act, 2023 can be found [here](#) and the implications for children's privacy [here](#).

At DeepStrat, we design privacy solutions, which include technologies, policies, and processes for becoming DPDP compliant. Contact us to know more.



The Telecommunications Act, 2023

The Telecommunications Act, 2023 was passed in the winter session of the Parliament. The new law subsumes three Acts – The Telegraph Act, 1885, Indian Wireless Telegraphy Act, 1933, and the Telegraph Wires (Unlawful Possession) Act, 1950, with the objective of development, expansion, and growth of the Indian telecom sector.

Undoubtedly, there was a need for replacing pre-colonial era laws and modernizing the regulatory framework for the sector. The Act attempts to do so through simplification of processes. It brings licensing, registration, and other permissions under one unified “authorization” for service providers to operate in India. This will do away with scores of licenses, permissions, etc. that the DoT earlier used to issue and mitigate tele-latency in under-served areas.

But there are also concerns with the Bill. Its broad definitions rang alarm bells among the industry about regulation of OTT communication services and telecom services under the same umbrella. Clarifications issued by the Ministry indicated that this law will only apply to telecom services. It is critical to maintain the distinction between carriage and content services across regulations. The latter is already regulated under the IT Act and Rules.

There are other concerns with the law, such as the mandate to conduct biometric authentication for telecom users. This provision will have to stand the test of Supreme Court’s Puttaswamy-II judgment. It will also have major privacy implications and its implementation will have to be checked against the DPDP Act. The Act also has provisions on surveillance and denial of internet access, which pose a risk to the fundamental rights of citizens.

Our submissions to the Ministry on the 2022 Draft of the Bill can be accessed [here](#). The current version of the law was passed without consultation.

Artificial Intelligence



The year saw a lot of activity in the AI policy space. The need for AI regulation also became stark as potential risks of AI became known and even market leaders in AI called for a halt to the AI race in the absence of proper guardrails.

The Global North has led in development of AI and policy. Prominent policies such as USA's Executive Order on AI and EU's AI Legislation were released in 2023. AI, however, has a global impact and therefore, its regulation has to be viewed from a global perspective.

It was a momentous year for India as it chaired the Global Partnership on AI, 2023. India used this opportunity to spearhead many policy and R&D initiatives throughout the year. The IndiaAI report, which lays down the foundation of India's AI Strategy, was released by MeitY. The strategy looks at optimisation of India's compute infrastructure, data, AI financing, research and innovation, targeted skilling, and institutional capacity for data to leverage the AI opportunity for India.

GPAI hosted a research symposium on advancing responsible AI in public-sector applications. DeepStrat's paper on "Regional inequities in extraction and flow of resources that support and power the design, development and access to AI: Experiences from India and Kenya" was selected to be presented at the [symposium](#).

The paper analysed the impact of industrialisation, colonisation and technology denial on the Global South. Investments in AI are centered in the Global North, making it the hub for AI development. India is one of the few countries from the Global South to have skin in the game. The region faces unique challenges such as lack of tech infrastructure, algorithmic biases, and migration of STEM workers. A combination of these factors underlines the need for the Global South to build regional cooperation to develop AI that can be leveraged for its priority sectors and retain its advantages within the region.



Cybersecurity

As the country's digital landscape grew, so did its attack surface. Some major cybersecurity breaches on critical sectors of India underscored the need for robust cybersecurity frameworks. At DeepStrat, we undertook several projects with the aim to facilitate collaboration between the regulators and industry to collectively enhance our cybersecurity posture.

We published our study on Cloud for Critical Information Infrastructure, which examined the advantages of the Cloud for securing the country's critical sectors, such as energy and power, health, and BFSI. We looked at these sectors because they are most sensitive from a national security standpoint and have been subject to growing attacks this year. The study looked at the evolution of cybersecurity doctrines, jurisdictional approaches of other countries and mapped India's policy against them. We found that moving to the Cloud offers increased security, cost optimisation, scalability, and ease of compliance. Consequently, there is a need for updating our policies to cater to the growing cybersecurity needs of the sector and to better safeguard the country against cyberattacks, while facilitating growth. Our study can be read [here](#).

We also collaborated with a major Internet Infrastructure Company to design cybersecurity workshops for info-sec professionals from the private and government sectors. Our first workshop was on the emerging DDoS threat landscape, where we looked at attack patterns, industries impacted and discussed mitigation measures to safeguard against this evolving threat.

Our second workshop will be in-person in January next year, where CERT-In will also participate to offer hands-on training on building a solid Zero Trust Architecture.

At DeepStrat, we undertake several cybersecurity projects where we help build technologies, policies, and solutions to safeguard against cybersecurity risks. Contact us to know more.



TRAI's proposal on Calling Name Presentation

The Telecom Regulatory Authority of India (TRAI) published a consultation paper on introduction of Calling Name Presentation (CNAP) in Telecommunication Networks to address the concerns of telecom users with respect to unsolicited commercial calls.

DeepStrat's submission in the consultation centered around three key issues. First, enabling Caller Identification for all users, without their consent, raises privacy concerns. This was especially risky in the absence of a privacy law earlier in the year. Second, the KYC process for acquiring SIM cards has met with many challenges, resulting in incomplete or inaccurate KYC data. We had highlighted these issues with the KYC process and its misuse by bad actors to commit cybercrimes in an earlier DeepStrat [study](#). Third, operationalising this framework would be met with infrastructural challenges, at a cost that does not justify the privacy and security risks associated with it.

Our submission to TRAI can be read [here](#). Our counter-comments can be read [here](#).

Cyber Crimes



In 2020, DeepStrat conducted a [study](#) in collaboration with the Haryana Police on Retail Financial Cyber Crimes in India. There were many findings in the study, which have been validated time and again. One of our findings was that cyber offenders work in collaboration and constantly evolve their techniques, tactics, and procedures, making them harder to catch. This calls for collaboration among the good actors to enhance capabilities and build proactive measures, instead of reacting to the problem.

This year we signed an MoU with Telangana Police, who are pioneers in their investigation of cybercrimes. We partnered with them to support research projects which would aid in investigation and suggest policy measures to mitigate certain challenges.

After studying the Telangana model, we also initiated the creation of a partnership between the police and the industry in our home state, Haryana. We based this on the Telangana model, which we believe is worth replicating in other states to build the collective capability of Law Enforcement Agencies.

In Haryana, we are helping the state police create a not-for-profit society, “Utkrisht”, to work towards the security and welfare of the state. It will be led by the Director General of Police of Haryana as its ex-officio Chief Patron, the ADGP as its Chairperson and a member from the Industry as its Convenor. The members will come from both the police and the industry. The Society is being built on a foundation of trust, partnership, and collaboration between the stakeholders. This project is currently in the pipeline.

Next year, we will start working on the Society’s initial focus areas – cybercrimes and cybersecurity, community-led policing, women’s safety and road safety. We are hopeful that our collective capabilities put together in a structured and targeted manner, will help solve many cyber and other issues, and help build a more secure infrastructure for the state.



Broadcasting Services (Regulation) Bill, 2023

The Ministry of Information and Broadcasting (MIB) released a draft Broadcasting Services (Regulation) Bill, 2023 for public consultation. The Bill will replace the Cable Television Networks (Regulation) Act, 2023, with its stated objective of streamlining the regulatory framework for various broadcasting services.

The Bill covers both traditional broadcasting services and OTT services, which has raised many concerns. There is an inherent distinction between the nature of these services, with broadcasting being a push service, while OTT is a pull service. Broadcasting is one-to-many, and therefore has a broader public impact, while OTT is one-to-one. These fundamental differences require different regulatory approaches for both. Regulating both in the same bracket would not only impact fundamental rights, but also hinder the growth of the OTT sector in India.

At DeepStrat, we prepared our submissions to the Ministry, which we will publish next year.



Digital India Bill

Lastly, MeitY undertook the significant task of replacing the IT Act of 2000 with a modern, principles-based and risks-respecting framework to regulate the new digital India. The need for a new IT legislation has been felt since the digital landscape has significantly changed from how it looked 24 years ago, with the emergence of new technologies and platforms, and the new opportunities and challenges that they have created.

In order to achieve the country's goal of becoming a trillion dollar digital economy by 2026, there is need for a modern and future-proof legislation that recognises and classifies new types of intermediaries and regulates them under a principles-based framework. The Ministry organised consultations on the new Digital India Bill, where they discussed the themes that will be covered under the law. Its objective will be to create an open, safe, trusted and accountable internet for digital nagriks, while accelerating growth of the innovation and technology ecosystem.

At DeepStrat, we did an in-depth [analysis](#) of the themes under the DIA and participated in the Ministry-led consultations. We examined how the law can tackle [intermediary classification and liability](#), [fair markets and innovation](#), [online harms](#), [emerging technologies](#) and [cybersecurity](#) and made our submissions to the Ministry.

The DIA will create a framework for the existing IT Rules, the DPDP Act, and the new criminal laws to work together in a manner that safeguards digital nagriks and catalyses growth of the digital economy. How will the framework regulate AI? How will the spread of mis/disinformation be checked in the upcoming election year? It will be interesting to see how this saga unfolds next year.



DEEPSTRAT

STRATEGY . POLICY . ACTION

 contact@deepstrat.in