Modi 3.0 and Digital India: Past, Present, Future

A report by Sapni G K

SUPPORTED BY

COMMON EDGE

The findings expressed in this report are those of the author and do not necessarily reflect the views of Common Edge

The story of digital technologies in India has taken the fast lane between 2014 and 2024. The acceleration of development of digital technology in general has contributed greatly to this shift. However, it is also indicative of the changing economic and political ambitions of the state. The extension of technology solutions certainly bled into the socio-cultural realities of the nation as well as the policymaking apparatus of the state, often tilting towards identifying technology as the solution to the ills of most challenges that the country faces in the 21st century. A stocktaking exercise of these changes and their effects is appropriate as Prime Minister Modi returns for a third term. It can be reasonably expected that digital technology policy decisions will certainly be a key area of focus under Modi 3.0.

Identifying the myriad policy shifts that have happened in the digital technologies realm over the last ten years under Modi, and spotting trends can help recognise the potential route that governance could take during the third term. This analysis aims to achieve that, while touching on the social, economic, political, and cultural impact of technology policy decisions. It anticipates what digital technology policy in Modi 3.0 could look like and therefore posits some hopes for improvements from the rights perspective. As this audit progresses, it also draws from analyses provided by other experts in the Indian digital technology policy space adding to its depth by not being limited to a single person perspective of technology policy landscape under the Modi years.

General trends from the last decade

A bird's eye view of digital tech policy decisions in the past decade helps identify a broad stroke of policy pathways that the government has adopted.

The centralization of policymaking on all things digital tops the list. During this period, legislative interventions have breezed through the Parliament with minimal scrutiny, and constitutional commitments to federalism have been overlooked. This can be a direct impact of the centralising nature of technologies that captured the 2010s. However, it does not excuse the nature of policy frameworks that govern digital data or digital technologies centralised. The various draft policies on digital health data exemplifies this. The digital architecture and policy framework around health, which remains a state subject under the Constitution of India, indicates the same. It has pushed policymaking towards union authorities and agencies, impacting federalism, limiting the autonomy of states as well as their decision-making abilities and ownership.

Over the last decade, digital health also serves as an example of the enthusiasm of the government to incorporate new digital technologies into governance and vision of the government. The different developments under the Ayushman Bharat Digital Mission, the national plan to develop digital health infrastructure, not only create a centralised system, but further extends the use of 14-digit unique health identification (UHID), which creates operational challenges in preserving privacy of extremely sensitive health data. Rolling out such technological architecture to large parts of the population, without adequate sandboxed pilots directly impacts the beneficiaries.

Building the India-stack technologies

Most technology-enabled welfare solutions in India stem from the Aadhaar experience. Aadhaar is a 12-digit unique identity number that every Indian resident can apply for. It is linked to biometric and demographic data, and can be used by residents to prove their identity and address details. Aadhaar was conceptualised as a way to reduce redundancies and corruption in the welfare system, however it has excluded plenty of rightful beneficiaries, often the extremely marginalised. UHID, Aadhaar and the famed Unified Payment Interface (UPI) all form part of India's vision of the India-stack model, creating alternatives to the big-tech dependent model. The first two Modi governments have been enthusiastic proponents of this model, exporting it to many other countries across the globe.

The minimal accountability for tech developed and used in government processes remains a concern. For example, some of the problems of Aadhaar could have been avoided with better audit and analysis within a sandbox environment, before full-fledged rollouts. New technologies and platforms created within the framework of Digital Public Infrastructure must tackle the challenges arising from policies that enable state monopolies. It should engage better with all stakeholders, including the key participants within the ecosystem and civil society organisations that demand greater transparency. It is also marked by the outsourcing of tech development and ownership to nonprofits and volunteer groups, which are not directly accountable to the citizens, as is the case with DigiYatra – the facial recognition system for contactless passenger processing.

The political will and enthusiasm for policymaking that supports Indian development of tech infrastructure is countered by the hesitation in engaging with a wide range of stakeholders and iron-fisted decision-making. Criticisms on the infrastructure or policy, such as those related to data security of DigiYatra or those on overtures of the data protection framework go unaddressed. Poor engagement with good faith actors manifests in the form of neglect, or is dismissed with strawman arguments that inadvertently attribute malice to the criticism without addressing the substance of it. It is also marked by great lethargy on law making, mimicking the global trends on the excruciatingly slow pace of legislating on digital rights. However, through the past decade, laws and subordinate legislation have watered down transparency and accountability of the state, as well as expanded the scope of unchecked state interference.

Specific imagery of Modi 1.0

The electoral campaign run by the Bharatiya Janata Party (BJP), to which Modi belongs has been at the forefront of utilising virtual space as early as 2012-13. Platforms such as Facebook, WhatsApp and X (then Twitter) were effectively utilised to mobilise cadre and political support. This pro-technology stance of the party leaders also translated into a pro-digital governance stance once the party came into power in 2014. The Aadhaar-based Direct Benefit remains the most significant example. Its architecture was legalised by the Aadhaar Act in 2016, but went through long drawn public debate challenging its constitutionality.

While the Supreme Court of India upheld the Act and the Aadhaar scheme, it also recognised the inherent right to privacy under the Constitution of India that the government was unwilling to recognise. Aadhaar continues to be the most defining piece of digital policy decisions of the last decade, which shifted the course of Indian digital rights related policy. It laid down the blueprint that continues to be explored and extended in various situations.

Net neutrality

While Aadhaar became a political contention across the Indian society, a major positive development on digital rights was also achieved during this period. In parallel to the United States Federal Communication Commission's (FCC) deliberations around repealing net neutrality, the Telecom Regulatory Authority of India (TRAI) also floated a consultation paper that seemed to water down net neutrality in India. Net neutrality is the concept that internet service providers treat all internet-based communications equally, without differentiating them on the basis of device, application or platform used and content consumed. After prolonged consultations and public campaigns, the Department of Telecommunications approved TRAI's pro-net neutrality recommendations, adopting an anti-zero-rating policy stance. This remains one of India's biggest digital rights policy successes to date.

New pastures of technology

The State-sponsored digital transformation continued, and the demonetisation exercise in 2016 was the next major project. Launched in April 2016 by the National Payments Corporation of

India (NPCI), UPI was designed to facilitate seamless, instant bank-to-bank transfers using mobile devices and the government's tech architecture. This innovation aimed to simplify digital transactions and promote a cashless economy, aligning with Modi's vision of a Digital India. Criticisms continue to pour over both the privacy related concerns of the UPI infrastructure as well as the state interference in markets. This was also the period that saw digitisation and digital architecture developed for sectors beyond finance, such as health. Finally, NITI Aayog, the government's think tank was also fairly on time to jump on the Artificial Intelligence bandwagon, coming out with its National AI strategy in 2018.

Cybersecurity and breaches

The first term of the Modi government, from 2014 to 2019, was also characterised by an unprecedented rise in data breaches. Large databases including the Aadhaar database, and the Nuclear Power Corporation of India Ltd suffered breaches, raising privacy and national security concerns. The absence of a data protection framework meant negligible obligations on the State as a data fiduciary. Poor investment, lack of awareness, outdated regulatory frameworks and weak accountability continue to be one of the key reasons for India's poor standing on cybersecurity indices.

Influence operations

The reducing costs of going online saw millions of Indians sign up to social media platforms. During the Modi 1.0 period, the public embraced the platforms without being aware of the potential to be manipulated or surveillance. Domestic influence operations became a characteristic during this period, with IT cells using private messaging apps including WhatsApp and Telegram, and public social media platforms such as Facebook, X (then Twitter) and YouTube to form narratives and shape public opinions. According to journalist Kumar Sambhav, the first term of the Modi government saw massive surrogate political campaigns that were rampant on Facebook, WhatsApp and Twitter. These influence operations were localised, gaining organic virality. Reports later revealed non-neutral stance taken by these platforms, including an expose about Facebook employees that worked with the BJP, often bending its community standards and platform rules to benefit Modi's party.

WhatsApp Lynchings

The Modi 1.0 period also coincided with a massive surge in online hate speech, which resulted in loss to life and property. WhatsApp lynchings, as they were called, were a spate of mob lynchings that happened because of misinformation spread through WhatsApp. The victims were mostly of marginalised identities – Dalits, Muslims, and people of tribal origins – who were targeted because rumours on Whatsapp claimed they were involved in child trafficking, cow smuggling, or theft. While government pushed for WhatsApp to take steps to curb these vigilante activities, the State apparatus mostly remained a spectator.

The Laws

Poor motivation to actively intervene on digital rights through concrete instruments of the state also reflected in the long-drawn deliberations on the Indian Data Protection Law. An exercise that began as early as 2017 with the recognition of the right to privacy by the Supreme Court of India, continued through the first term of the Modi government. Other efforts on policymaking such as protection of digital health data were also stalled. The deprioritisation of rights could also be observed from the various other state measures such as the rise of censorship and internet shutdowns using provisions under the Information Technology Act (IT Act), which allows the government to use unreasoned and unpublished orders. Cumulatively, the push for development and use of digital infrastructure was at an all time high, but the safeguards for it were lagging far behind.

Technology Policy Under Modi 2.0

The second term of the Modi government which commenced in 2019 was characterised by multiple major policy decisions that have left long-lasting impacts on Indian public policy and society.

The abrogation of Article 370 during Prime Minister Narendra Modi's second term was pivotal in India's political landscape. Article 370 granted special autonomy to the state of Jammu and Kashmir, allowing it to have its own constitution and decision-making powers over all matters except foreign affairs, defence, finance, and communications. On August 5, 2019, the Modi government revoked this special status, effectively integrating Jammu and Kashmir more directly into India's federal framework.

The abrogation of Article 370 impacted the civil and political rights of the people of Jammu and Kashmir, who had enjoyed special rights that were guaranteed by the Constitution due to the nature of their accession to the Indian union. It also challenged the federal aspects of the Constitution of India. On the digital rights front, a complete blackout of internet services commenced in August 2019, effectively rendering it one of the longest internet shutdowns ever recorded. It was partially restored in January, 2020 enabling access only through archaic and extremely slow 2G services. The Supreme Court of India criticised indefinite internet shutdowns based on arbitrary and secretive orders passed under Section 69A of the IT Act, calling for more transparency but stopping short of mandating the government mend its ways. Gyan Tripathi, Fellow at SFLC.in quips that the Indian government has perfected the art of internet shutdowns, highlighting how the government continues to use it as a tool, despite a lack of concrete evidence on what it achieves and overwhelming literature on the monetary and opportunity costs to the public. Technologist and interdisciplinary researcher Rohini Lakshane flags that her research has suggested that shutdowns further exacerbate the challenges faced by women, a perspective that is often missed while analysing internet shutdowns.

Accelerated Datafication

Early in 2020, a decision by the Ministry of Highways and Road Transport to monetize the data in the Vaahan-database came to the limelight. The database hosted information about vehicles registered across the country. The Ministry was sharing granular details to private parties for a price, without the consent of the concerned data principals. This, combined with the almost mandatory FasTag – the Radio Frequency Identification system for toll collection, meant that sensitive information about millions of Indians was up for grabs with next to zero protections or any informed consent. The absence of a data protection law continued to limit any effective action to protect citizen interests. Researcher

Shraddha Mahilkar highlights that the conceptualisation of data as an asset for exploitation and profit sees data as separate from how it affects bodies and the physical world. This, coupled with other actions of the government aiming to modernise and improve governance, she says, have often disproportionately reinforced existing inequalities for historically marginalised communities. Mahilkar emphasises that data breaches have put them at risk of exploitation, coercion, and discrimination, often with little recourse due to inadequate legal frameworks. Women from these communities, already facing systemic violence and oppression, are particularly vulnerable to such breaches.

COVID-19 and surveillance

Like many countries across the globe, digital rights policy making took a distinct turn during the coronavirus pandemic. Surveillance systems were embedded into contact tracing apps to track and enforce quarantine during the pandemic. India's Aarogya Setu was developed by volunteers and guided by a data access and knowledge protocol, which did not recognise grounds for effectively contesting the misuse of data, even when read with the penal provisions under India’s Disaster Management Act, 2005. The setting up of such an extensive public surveillance architecture under the cover of developing digital health solutions endangered privacy and digital security and undermined a host of other readings of fundamental rights protected by the Constitution of India. However, techno-solutionism seems to have lost this battle in 2023, when Aarogya Setu’s data access and sharing protocol was discontinued, contact tracing feature deleted and all the contact tracing data was admitted to have been deleted.

Platform politics

Modi 2.0 saw some radical decision-making on platforms at large – almost all of them that fell within the ambit of ‘intermediary’ under the IT Act. While some of these decisions, such as policy positions around Telecom and Internet Service Providers which directly affect access to the internet, could be traced back to Modi 1.0, other policy decisions, including laws were made under Modi 2.0. The first of these related to the ban on TikTok and 58 other Chinese apps in India, following geopolitical skirmishes along the border shared with China. The overnight ban particularly impacted the lives of content creators primarily from semi-urban and rural areas in the county who had found their livelihoods on the app. This move was criticised by multiple stakeholders, including its impact on international rules on market access, but ultimately made India the first amongst many countries to ban Chinese apps based on cybersecurity concerns.

Digital Rights in Fintech

Similar concerns also led to the shutdown of operations of a host of Chinese loan apps. They were posing major challenges to users and regulators, as these poorly regulated lenders were often pushing users into large debt traps. This analysis does not delve deep into the digital rights-related decisions in the finance domain, but it is important to acknowledge the operation of loan apps funded by Chinese companies that created regulatory and social challenges, which pushed India’s Central bank to create stricter norms for financial transactions in the digital realm, which is also reflected in India’s approach to cryptocurrencies as well. However, real money-based betting and online platforms that facilitated the same received a much better treatment from the policymakers. Even when some states banned the operation of these platforms citing their business models mimicking gambling, the Union took a more laissez-faire approach to policy making on online gaming.

Intermediary Liability

India has been following the American interpretation of the 'safe harbour' law to consider online intermediaries as mere conduits and not active participants in user-generated content on platforms. However, there is a visible shift in this approach now, attributable to tech policymaking under Modi 2.0. The expectation of active interference by the intermediary, especially social media and messaging platforms had already been on the rise. This also resulted in a spike in censorship – both through takedowns at the behest of government blocking orders as well as by platforms themselves, as an anticipatory measure to prevent liability. This trend was concretized by the passing of the Information Technologies (Intermediary Guidelines and Digital Ethics Code) 2021, which not only expanded the power of the Union government over platforms, but also extended many new stipulations on digital content - including news media, content available on over-the-top platforms (video streaming), and user-generated content. These rules were further amended in 2023 to further deepen the grasp of the Union government on speech and expression in the digital sphere, where it mandated the establishment of government fact-checking units and further tightened the noose around content takedown by intermediaries. These changes in policy operated alongside Section 69A of the 1T Act, which continues to allow unreasoned and secretive takedown orders, bereft of transparency and accountability.

Women on the Indian internet

A cursory analysis of the experience of women on the Indian internet would suggest that it has deteriorated through these years. Armies of real and fake profiles attacked women who expressed unpopular and critical opinions, with little consequence. This trend was empowered by ruling party supporters who resorted to name-calling, rape and death threats, and continued mental harassment of women who used the platforms at their disposal to air their views. The Ministry of Home Affairs together with the Ministry of Women and Child Development developed the Scheme for Cyber Crimes Prevention against Women and Children. The National Commission of Women also launched a WhatsApp helpline for women experiencing domestic violence. However, as Rohini Lakshane highlights, there is no data about the uptake of these services from the government. The lack of transparency makes it difficult to meaningfully analyse or engage with these measures. The track-record of successive Modi governments does not shine bright, as Lakshane points at the poor implementation of the IT Act, which she says "focused on morality, decency etc and does not put victim-survivors front and centre."

The gendered experience of the internet was further exacerbated for human rights defenders and journalists, who were mercilessly trolled and attacked for challenging the dominant narrative of governments, religions, and caste. This was particularly pronounced during the protests against the citizenship Amendment Bills and the Farmer's protests in India during Modi 2.0. Public sentiment had been influenced to an extend that any criticism of violent exhibition of Hindutva or supporting a person following Islam could lead to death threats and rape threats, even on infants. These were clear instances where more sophisticated influence operations on digital media played out. As Kumar Sambhav explains, these localised operations were getting more difficult to detect as the networks of WhatsApp groups and communities and the circulation of content in such networks were managed more centrally by influence groups. While WhatsApp continues to be a popular medium, influencing in general seems to have shifted from Facebook, and Twitter to YouTube, Instagram and Telegram.

Lateral Surveillance

During this period, an anti-protest sentiment also developed in the county, which was supported by policy measures such as the introduction of lateral surveillance programmes such as the Cyber Crime Volunteer program. Within this 'anti-protestor' context, it is unsurprising that Amnesty Security Lab's research found the illegal use of Pegasus spyware on the mobile devices of political leaders and human-rights defenders in India. The Union government brushed aside the investigation as baseless, and did not take any measures to improve the oversight and accountability mechanisms on surveillance, interception, and monitoring in India.

New Legal Regimes

The passing of the Telecommunications Act, 2023 only broadens the scope of government actions, with poor oversight, transparency, and accountability. The potential challenges it brings to encryption will continue to affect marginalised sections of the society more than it affects others. This includes further censorship of marginalised people including women and heightened self-censorship in digital spaces. The prevalence of deep fakes and AI-based tools that distort content, further adds to the reasons for worry, which the mere publication of unenforceable advisories and guidelines cannot mitigate. The draft Broadcasting Bill, 2023 which sought to replace the Cable Television Network (Regulation) Act, 1995 also added to policymaking that could further censorship and government overture into freedom of speech. It extended to the digital sphere with its broad definition of what could be considered a “broadcasting service”, by including everything from content streaming platforms and digital news media outlets to online current affairs content creators, greatly restricting the exercise of online free speech and journalistic freedom.

Technology-related lawmaking in India saw its most significant piece of legislation passed during Modi 2.0. The Digital Personal Data Protection Act (DPDP) was finally passed in 2023, after deliberations and multiple iterations over a span of seven years. The Act has been widely criticised for the sweeping exemptions to the government from obligations towards data principals. Compared to the earlier drafts from 2018 and 2019, the DPDP watered down protections for the data principals. It weakened the constitution of the Data Protection Authority, which is now acutely dependent on the Union Government. However, even with an inordinate delay in its enactment and immense scope for improvement, the law gets the ball rolling on data protection and enforcement of some aspects of privacy in India.

Towards the end of its term, Modi 2.0 also delved into policymaking on the competition-related aspects of digital technologies and digital markets. In its interest to protect market fairness, market integrity and consumer interests to support effective realisation of digital rights, it published the draft Digital Competition Bill, 2024. It is a useful starting point to minimise concentration of power in digital markets, especially with the advent of centralising technologies such as AI. Further deliberations on the proposed Bill should iron out blind spots such as consideration for rights of platform workers such as content creators and gig labourers in multi-sided digital markets. Instead of being the final authority on tech policymaking, the Union government should support the creation of an empowered regulator which has the expertise to make digital competition policies.

What would technology Policy look like under Modi 3.0?

Surprising many pundits, Modi's re-election for a third term comes in coalition, and not by a brute force majority of the BJP. The regional parties that supported the formation of the Union Government and a stronger opposition will hopefully shift tech policies to be more rights-respecting. There is also an opportunity for India to contribute to global digital rights challenges, as it once did with net neutrality.

DPI and the world

As it did during its G-20 presidency, India will continue to popularise the Digital Public Infrastructure (DPI) rhetoric and the India-stack model, which will continue to expand horizontally across sectors. The exact definition of what constitutes a DPI is elusive, as its broad scope covers every digital service that could be offered by the State, international organisations or even private players. However, India has been the experimentation ground for government supported digital infrastructure and tools, and it wants to take a lead on this movement globally. The Indo-Sri Lankan agreement to implement an India-funded Aadhaar-like biometric identity system run on the Modular Open-Source Identification Platform (MOSIP) in Sri Lanka, alongside six other countries rolling out biometric identity projects run on India's MOSIP is a testament to India's interest in this space. Public policy researcher Smriti Parsheera cautions that achieving scale in such projects cannot be prioritised at the cost of individual liberty and free choice. Exporting the philosophy of DPIs and the locally developed tools will form part of India's soft power arsenal in a world that is changing rapidly due to technology and is constantly looking for non-big tech alternatives. As Parsheera highlights, the world needs to be aware of the competition policy impact of creating state-backed monopoly infrastructures, as they pose the jeopardy of emerging as 'alt big tech' players in the digital ecosystem.

We will continue to see India push such alternatives locally as well, focusing on policy-level support for indigenous development of alternatives to frontier technologies. The motivations, however, are clear in their efforts to make digital technologies more language inclusive to improve both access to digital technologies and protecting some of the many languages used in the country.

What about AI?

The July 2024 Budget speech by the finance minister, the most recent policy document from the Union Government did not mention 'artificial intelligence'. This might be indicative of an intrinsic awareness about the hype around AI. However, this might not stop the integration of more AI based tools into government services, and reshape the imagination of governance technologies. Sambhav highlights the government's plan to improve delivery of the government services by collecting, digitising and standardizing citizen's records, building interoperable databases and integrating AI for algorithmic decision making. He cautions potential instances of citizens' data being smoothly shared between government agencies and ruling parties and government agencies and private industries without citizens having much say in it, and therefore calls for better legal protections.

A new AI policy is in the works, which is expected to further push the government's innovation narrative. Digital rights defenders will need to interrogate this policy, as it will lay the groundwork for the use of AI technologies in the country, which would most likely increase the levels of surveillance across digital and physical spaces.

More laws on platforms?

Encryption, data protection, platform regulation and content moderation will also see new developments soon, as subordinate legislations under the DPDP Act are released. Parsheera also shares how these rules have to be a top priority for the government at this point, and that it must ensure a deliberative process to formulate the rules needed to give effect to different aspects of the law while revisiting the issue of data processing by law enforcement and surveillance agencies in its current iteration. The vacuum created by the overhaul of the criminal codes in the county could also create challenges as new interpretations of the law emerge, challenging established norms that will also affect the digital sphere. Mahilkar also adds the lack of intersectionality in policymaking and the digital divide to the list of concerns that can significantly harm Dalits and indigenous people. As a young person, Gyan Tripathi also echoes that the discernible gap between the ambitious goals set by digital policies and their on-ground implementation due to inherent inefficiencies, lack of local-level infrastructure, and insufficient funding greatly challenge aspirations of the country's youth in "Digital India".

Platform Labour

The rights of gig workers navigating labour through digital platforms is often sidelined in mainstream conversations about technology policy. The Labour Codes enacted under Modi 2.0 did little to protect these workers and their rights as the digital economy brought in new challenges to worker rights. Advocacy by gig workers across the spectrum has now moved the needle, and multiple state governments are in the process of enacting legislations that marginally improve the legal recourse available to these workers, who are otherwise at the mercy of aggregator companies. The Union government could follow the multiple state governments which have started taking a proactive stance on digital labour rights. The digital rights of workers engaged in platform labour, affecting the physical manifestations such as exploitation facilitated by black box algorithmic decision making and virtual rights such as ownership of self-generated data, are more likely to get policy attention under Modi 3.0.

A different Digital India

While a feminist internet might not even be a remote consideration for the government, the rhetoric of protection of women and children could be used, as it is in other parts of the world, to restrict digital rights and the use of digital technologies without adequate reasoning. The proposed Digital India Act hence warrants much attention from the global human rights community. As Parsheera urges, meaningful consultations, and reasoned decision-making in response to those inputs should be key considerations as the law is likely to bear significant influence on digital rights in India, across areas like censorship, automated decision-making and meaningful redress. Good-faith consultations and responses to the inputs are imperative to advance digital rights in India, and taking public criticism to shelf unwelcome proposals, as was done in the case of the draft Broadcast Bill, 2024 is a trend that will help advance digital rights as tech policy decisions are made during Modi 3.0.

Sapni G K is a lawyer and public policy researcher studying the intersection of technology, law, policy, and society.