Regulating New Technologies: Three Central Principles

ANANTH PADMANABHAN

Technology has significantly driven India's growth over the past decade. Be it the rise of well-funded startups and 'unicorns', the imaginative use of technology for governance, or the emergence of India as a hub for R&D activity and a test bed for product innovation, technology is an important driver for growth in India. A 2018 report by the Startup India Initiative states: 'The ecosystem comprises of over 14,600+ Startups, approximately 270 incubation & business acceleration programs, 200 global & domestic VC firms supporting home-grown Startups, and a fast-growing community of 231 angel investors and 8 angel networks. India also boasts of being home to the 3rd largest unicorn community, with over 16 high valued Startups having raised over $17.27 billion funding, with overall valuation of over $58 billion."[1]

But with this exponential growth comes a set of policy and regulatory challenges. First, government policy and the regulatory framework need to be aligned to enable the growth of a robust technological ecosystem, rather than impede it. The global competition for leadership positions in emerging technology domains, such as artificial intelligence, drones, gene editing and other areas, has become aggressive, with China becoming a lead contender. This global race demands impactful innovation policies that ease up creative and inventive activity, but in a responsible manner.

Second, as various incidents post 2016 demonstrate, the rise of the digital has created new vulnerabilities and new types of harm to individual and group rights. A digitally connected ecosystem is rife with security concerns, which are exacerbated when digital literacy

does not keep pace with digital use. Moreover, with personal data becoming a critical tool for monetization and profiling, the incentive for both industry actors and the state to secure such data and respect individual privacy is quite low. Both the Facebook–Cambridge Analytica controversy and the unrestricted seeding of Aadhaar data in multiple databases to build a 360-degree view of citizens indicate distinctive kinds of threats to individual and community rights. Therefore, respect for privacy and individual/community rights must be externally imposed, with regulations playing a part in this process.[2] In short, developing an indigenous regulatory framework for new technologies is a pressing need for India. Three central principles are integral to this transition.

Three Central Principles

The first principle for regulators and policymakers to bear in mind is **clear identification of the problem that regulation must address**. While this is not unique to the technology context, there are a few specificities in this field that make this principle worth emphasizing. Often, technological change affects sectors that are under an existing regulatory apparatus, as seen in the case of online cab aggregators or food delivery services. When regulators attempt to transplant this apparatus to a new factual reality, a common mistake is to assume that regulations must address the same set of problems as witnessed in the earlier non-tech scenario. But in doing so, the regulatory response addresses more problems than required, because technology-enabled models are likely to sort out at least some concerns.[3] This response also presents the danger of under-inclusion as new challenges raised by technology-based models may be missed in the process. Therefore, it is imperative to clearly identify surviving and new problems caused by technology, separate those that demand immediate regulatory attention from others that may only require a wait-and-see approach, and then develop targeted regulatory and monitoring strategies for each of these concerns.

For instance, the draft e-commerce policy released for discussion in 2019 defines 'e-commerce' as including 'buying, selling, marketing or distribution of (i) goods, including digital products and (ii) services; through electronic network'. Evidently, this is an extremely wide definition that brings within regulatory control a wide range of activities from online retail to app-based health delivery. The document also attempts to outline policy for a host of different problems: data; infrastructure development; e-commerce marketplace regulations such as anti-counterfeiting, anti-piracy and foreign direct investment; consumer protection; payment related issues; export promotion; and content liability exemption, among others. The concerns of social media are far removed from fashion retail, and consumer woes pertaining to online travel booking differ vastly from digital health solutions.[4] The unfortunate result is a heavily diluted effort that portends regulatory overreach. To avoid this in the future, regulatory approach must shift course from deciding in advance the range of business activities that need regulation to identifying the specific problems that proposed regulations must address, under the first principle discussed above. Inability to do so would only cause apprehension and uncertainty for businesses, and extremely ineffective and diluted protection for citizens.

The second principle is to **prioritize a risk-based and responsive regulatory approach**. When regulating unfamiliar territory, as is mostly the case with new technologies, proclivities to entirely ban an activity or create restrictive pre-activity licensing models are high. The bureaucratic instinct to play safe and apply a 'precautionary principle' comes at the cost of innovation and entrepreneurship.[5] Moreover, because many new technologies have cross-cutting impact, even these decisions are taken in silos with one agency or regulator taking a more pro-technology view while another acts more restrictively.

The changing stance on data localization in India suffers from failure to adopt such a risk-based approach. At the heart of this debate is whether private entities must be compelled to store the data of Indian citizens in servers located within India. A compelling rationale offered in support of this measure is that law enforcement officials find it difficult to investigate criminal misconduct when data resides in servers located else-

where. Another rationale offered is the threat to national security because of the possibility that foreign governments can spy on Indian citizens, taking advantage of the fact that their data resides in servers within their jurisdictions. A third rationale argues that localization can help advance a domestic artificial intelligence and data ecosystem, as done by China previously.[6] But amidst these multiple narratives, there is no clear study from the Government of India or any of the regulators about the extent of harm caused because of servers residing outside India, the less restrictive measures that could equally address any of these concerns.

To address these concerns, the regulation of emerging technologies should be risk-based and responsive. This new approach involves detecting undesirable or non-compliant behaviour, responding to that behaviour by developing tools and strategies, enforcing those tools and strategies on the ground, assessing their success or failure, and modifying approaches accordingly.[7] By valuing these processes, the overall approach towards regulation changes in an organic manner. Risk assessment involves multi-stakeholder conversations and an engagement with data that goes beyond projected fears and growth narratives. It entails creating a mechanism meant to gather the requisite information, including engagement with technical bodies. Finally, it also brings about some consensus among different regulatory bodies regarding the kind of enquiry involved, if not the answers to such enquiry. A healthy debate on the risks surrounding a new technology is essential for the creation of a proportionate regulatory framework that balances innovation and protection effectively.

The third principle is to **value democratic principles and fundamental rights**. The rise of the Internet and digital technologies has resulted in a loss of traditional state power and authority, leading to reassertion of control on the part of the bureaucracy. This reassertion now presents itself in the form of various regulatory controls such as demands to keep the privacy baseline low so that the state can easily access private communications, attempts to monitor online speech and to impose criminal and civil liabilities upon those expressing unpopular or undesirable views, and restrictive business requirements on private actors such as data localization. These controls, increasingly justified on the basis that China has relied on similar interventions to successfully build its innovation ecosystem, carry extremely harmful consequences for the future of democracy in India.

While many of governmental interventions do not come from a place of mala fide intent, it is important to be reminded often, as a polity, and especially so for policymakers and regulators, that India is built on a foundation of democratic values and crucial constitutional safeguards. As our experience with Section 66A of the Information Technology Act, 2000 – subsequently struck down by the Supreme Court in *Shreya Singhal* v. *Union of India*[8] – demonstrates, the impetus to regulate online behaviour or technological innovation should not emanate from a deep-seated desire to command and control. Such a desire is likely to result in unconstitutional behaviour and impermissible inroads into the fundamental rights of citizens, including free speech and expression and the freedom to do business. While realities such as the virality of fake news in the age of social media raise serious concerns, responses cannot be built on the assumption that a strong state (like China) can put a stop to these concerns. Moreover, often responses of this kind change the very dynamic of citizen-state engagement in a democracy, leading to possible misuse and a surveillance architecture that evokes fear.

Recommendations

The regulatory interventions coinciding with India's period of technology-led growth have been a mixed bag. Privacy may have found its ally in the Indian Supreme Court, but the data protection bill has long been in the works without much-needed push from the government to formalize it as a legislation.[9] Moreover, many of the safeguards against misuse of Aadhaar data, emphasized by the Supreme Court when upholding the validity of the Aadhaar Act, have been watered down through a recent ordinance that bypassed legislative scrutiny.[10] The data localization debates reveal uncoordinated action between different power centres within

the government, resulting in both business unpredictability and the fear of censorship through architectural changes to the Internet. Recent proposals in the realms of e-commerce and intermediary liabilities do not indicate well-thought-out measures of regulation that factor in the capacity for enforcement, the impact on fundamental freedoms including speech and business autonomy, or the proportionality of state action.[11]

Yet, there have been some green shoots as well. The drone policy is one such, coming as it did from a place of outright ban on the technology in 2014 to a state-of-the-art reg-tech solutions like Digital Sky and Regulations 1.0, in 2018, that leave room for further iterations that match the pace of technological advances in this sector.[12] The Telecom Regulatory Authority of India's position on net neutrality has been largely well received across the range of different stakeholders. On digital payments, the government has displayed considerable sensitivity towards various concerns ranging from innovation in the sector to consumer dispute redressal mechanisms and competition concerns. In all these cases, what comes through is some degree of mindfulness to the central principles outlined here. The government should now build on these early successes to develop appropriate regulatory toolkits.

Any regulatory intervention in the field of technology policy must begin with an insistence on a clear outlining of the harms involved and a mapping of the various alternate policy measures that could be potentially taken to address these harms. This is a good starting point for citizens and other stakeholders to develop awareness of the challenges that the state wishes to address, and the fit between these challenges and the proposed regulatory measures. The European Union has insisted on similar measures as part of its 'Better Regulation' principles.[13] The responsibility cast on the regulator to explain why it is regulating in the manner it proposes can make a significant contribution towards providing certainty, accountability and curbs on arbitrary intervention.

Regulation of new technologies should also enable experimentation with bespoke regulatory approaches and tools, as well as with innovative market solutions, both in a contained low-risk environment. 'Experimental regulation' seeks to achieve this objective by providing exceptions to, or exemptions from, existing regulation in a ring-fenced environment.[14] In many countries, experimental regulation has taken the form of sandboxing schemes. The UK Financial Conduct Authority's Project Innovate is a live example of regulatory sandboxing for financial technologies. Other jurisdictions such as Australia, Singapore, Switzerland, Hong Kong, Thailand, Abu Dhabi and Malaysia have also been experimenting with similar initiatives.[15] India needs to create more comprehensive thinking across multiple regulators about the efficacy and modalities of such regulatory sandboxes.

As many of the new technologies cannot be confined in clear terms to the regulatory jurisdiction of any one regulator, India also needs to develop strategies for better inter-agency coordination. The data localization controversy revealed how different regulatory and recommendatory bodies were at odds with each other on how to address this issue. Because data is a cross-cutting asset across multiple sectors, it is imperative to build better coordination and some uniformity in decision-making on matters of data governance. In the US, the Obama administration had created an Emerging Technologies Interagency Policy Coordination Committee to tackle the problem of siloed decision-making. Israel has established an inter-agency team to coordinate regulation of virtual assets. India must learn from these exercises and build a more coordinated regulatory strategy for data governance as well as other realms of new technology.

Finally, important regulatory interventions should also carry the mandatory requirement of a rights impact assessment. The current relationship between regulators and civil society is mostly one of direct acrimony and distrust, especially when it comes to regulating the Internet and digital technologies. The only way to usher in a structured change is to mandate a clear rights impact assessment, where the regulator must necessarily gauge the implications of the proposed regulatory approach on fundamental and human rights. Many instances of excessive and harsh regulations can be pre-empted at an early stage if this mechanism is built into the regulatory process.

END NOTES

1. 'States' Startup Ranking 2018' (New Delhi: Department of Industrial Policy & Promotion, 2018), 7-8, https://www.startupindia.gov.in/content/dam/invest-india/compendium/Startup%20India%20-%20National%20report_Final%20Version_web.pdf.

2. Alvin Chang, 'The Facebook and Cambridge Analytica Scandal, explained with a simple diagram', *Vox*, 2 May 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram; Rachna Khaira et al., 'UIDAI's Aadhaar software hacked, ID database compromised, experts confirm', *Huffington Post* (11 September 2018), https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/.

3. Ryan Hagemann, 'A regulatory framework for emerging technologies', *1776*, 16 March 2016, athttps://www.1776.vc/insights/regulation-emerging-technology-government-drones-hyperloop/.

4. See Ananth Padmanabhan and Arjun Sinha, 'White Paper on Regulating E-Commerce in India: Need for a Principles-based Approach' (New Delhi: Centre for Policy Research, 2019), http://www.cprindia.org/research/reports/white-paper-regulating-e-commerce-india-need-principles-based-approach.

5. Darcy Allen and Chris Berg, 'Regulation and Technological Change', in *Australia's Red Tape Crisis*, edited by Darcy Allen and Chris Berg, 218, 226-227 (Queensland, AU: Connor Court Publishing, 2018).

6. Compare, in this regard, the Reserve Bank of India Directive RBI/2017-18/153 dated 6 April 2018 with the draft National E-Commerce Policy.

7. Julia Black and Robert Baldwin, 'Really Responsive Risk-based Regulation', *Law & Policy* 32(2) (2010): 181.

8. (2015) 5 SCC 1.

9. *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1; Surabhi Agarwal, 'Personal Data Protection Bill only after new government takes over', *Economic Times*, 4 January 2019, https://economictimes.indiatimes.com/tech/internet/personal-data-protection-bill-only-after-new-government-takes-over/articleshow/67374919.cms.

10. *K.S. Puttaswamy* v. *Union of India* (2019) 1 SCC 1; Zaheer Merchant, 'Supreme Court refuses to entertain challenge to Aadhaar ordinance, tells petitioners to approach High Court', *Medianama*, 8 April 2019, https://www.medianama.com/2019/04/223-supreme-court-refuses-to-entertain-challenge-to-aadhaar-ordinance-tells-petitioners-to-approach-high-court/.

11. See 'Draft National E-Commerce Policy: India's Data for India's Development' (New Delhi: Department of Industrial Policy and Promotion, 2019), https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf; 'Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018' (New Delhi: Ministry of Electronics and Information Technology, 2018), https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

12. 'Civil Aviation Requirements', Series X, Part I, Issue I: Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS), F. No. 05-13/2014-AED Vol. IV (New Delhi: Directorate General of Civil Aviation, 2018), http://dgca.nic.in/cars/d3x-x1.pdf.

13. 'Better Regulation Toolbox' (European Commission, 2017), http://ec.europa.eu/smart-regulation/guidelines/docs/br_toolbox_en.pdf.

14. Sofia Ranchordas, 'Innovation-Friendly Regulation: The Sunset of Regulation, The Sunrise of Innovation', *Jurimetrics* 201 (2015): 55.

15. *Regulatory Sandbox: Making India a Global Fintech Hub* (Deloitte, 2017), available at https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-fintech-regulatory-sandbox-web.pdf.