Regulating Emerging Technologies in India: Challenges and Recommendations

Archana Sivasubramanian & Abhishek Chakravarty

Abstract

The sudden emergence of new technologies can always put governments and regulators in a space of perplexity. In India, while there is an immediate need to pass legislations or prescribe guidelines to regulate these emerging technologies, there also remains a deep vacuum in regulatory thinking. These vacuums are temporarily filled through regulatory approaches that do not further the innovation ecosystem while also not delivering public value and purpose. First, most regulations in India are 'command and control', in that they seek to enforce rules for companies and consumers alike, pushing a regime of excessive compliance. Second, these regulations are also need based and they develop impetuously when there is some public traction. This suddenness in regulations can be problematic for a healthy development of an ecosystem where innovation and purpose find instrumental value through rules and guidelines. Third, Indian regulators neither seek to understand the technologies they regulate, nor do they adequately pay attention to public needs such as privacy, algorithmic harms, legal liabilities and democratic values. They are more 'state-focussed' than 'public-focussed'. By this we mean that regulators seek to further and enhance state interests as opposed to furthering public innovation and purpose.

In this paper, we attempt to trace three major challenges in India's regulatory landscape, we then supplement it with a case study on the drone regulatory ecosystem in the country, and we lay out a unique framework for regulators to strengthen state capacity and rethink their approaches for India in the emerging technologies landscape. We also recommend an adaptive, co-regulatory approach for them to find the right balance in safeguarding interests of the state, enhance ease of doing business, promote democratic rights and encourage innovation that benefits the universe of emerging technologies.

Keywords

Regulation of emerging technologies; Drones; Legal liability; Privacy; Co-regulation; Theories of regulation; State capacity; Democratic rights; Algorithmic harms.

1.1 Introduction

The modern regulatory state has its focus on governance than government.[1]
Growing regulation pushed governments to a supporting role, while the civil society, in the driver's seat, "policed" business activities[2]. But it is not that the modern regulatory state has been very successful. This was very evident during the COVID-19 pandemic, when capacities of states across the world failed to achieve their goals to deliver public service. This vacuum in the governmental capacity of public agencies is a by-product of neoliberal market forces that led to minimum government. This development, in parallel, also led to the rise of the regulatory state where public institutions have taken the role of a regulator, intervening only in the functioning of markets through rules and guidelines. The role of the regulatory state has been to monitor and sanction, set standards for effective regulation and ensure compliance by private actors to the regulatory sanctions.

In India, regulators have taken on the policy making role to really develop policy pathways in the ecosystems they intervene. This norm is no different for emerging technologies, an area where Indian regulator continue to face a complex set of challenges. First, the question of what to regulate has a bearing over the question on how to regulate emerging technologies. Technological innovation is dynamic and unpredictable, and hence the emergence of new technologies is unforeseen. Indian regulators haven't solved the problem of what to regulate when it comes to emerging technologies over how to regulate them. Even while regulating these emerging technologies, the state's responses have been mostly knee-jerk[3]. Second, the kind of regulatory goals that the state has when it comes to regulating emerging technologies is not clear. Another development that should be factored in when considering regulating emerging technologies is the political economy of the state. The growth of foreign-owned digital businesses and foreign-funded innovations is in collusion with an emerging "Aatmanirbhar Bharat"[4] narrative, the narrative of self-sufficiency. Third, the state is unable

[1] Poul F. Kjaer & Antje Vetterlein (2018) Regulatory governance: rules, resistance and responsibility,Contemporary Politics, 24:5, 497-506, DOI: 10.1080/13569775.2018.1452527
[2] Kourula, A., Moon, J., Salles-Djelic, M.-L., & Wickert, C. (2019). New Roles of Government in the Governance of Business Conduct: Implications for Management and Organizational Research. *Organization Studies*, *40*(8), 1101 1123. https://doi.org/10.1177/0170840619852142
[3] See also elaborate on this in Section 2, under drone regulations
[4] Government of India, https://aatmanirbharbharat.mygov.in

to play catch up with emerging technologies. On the one side, India is still to even get a law to protect personal data but the state, on the other side, the country is attempting to regulate drones, cryptocurrencies and bitcoins without a clear, connected data governance framework and vision.

Regulating emerging technologies in India is of urgent and necessary interest because of the scale of innovation in the Indian technology ecosystem. Start-ups in India are locating new avenues of technological expression. A 2018 report by the Start-up India Initiative states[5]: 'The ecosystem comprises of over 14,600+ Start-ups, approximately 270 incubation & business acceleration programs, 200 global & domestic VC firms supporting homegrown Start-ups, 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 Start-ups having raised over $17.27 billion funding, with overall valuation of over $58 billion'. But there is still a need for an effective regulatory framework to tackle the policy challenges posed by the emergence of dynamic innovations in the technology space.

1.2 Three challenges in India's regulatory approach to emerging technologies

The first and a major challenge for India's regulatory state in the emerging technology landscape is the dynamic nature of this space itself. There is an ongoing tension between regulation and innovation in that the state must ensure adequate competition and create market structures that enable innovation, but the state also needs to regulate the new markets and check for anti-competitive concerns, and other democratic harms. As new technologies come to the fore, this tension is markedly visible in India. For example, there is a speculation that India will ban cryptocurrencies, but it is also argued that this will lead to dire consequences for India's economy.[6] A four-member committee headed by the former finance secretary, Subhash Chandra Garg, has put out a report in the

[5] "States' Startup Ranking 2018". (New Delhi: Department of Industrial Policy & Promotion, 2018), 7-8, https://www.startupindia.gov.in/content/dam/invest-india/compendium/Star...

[6] Rajagopalan, S. 2021. "India Bitcoin Ban would be a Terrible Idea". *Bloomberg* https://www.bloomberg.com/opinion/articles/2021-03-19/bitcoin-ban-proposed-in-india-is-a-bad-idea

public domain that advises the government to ban private cryptocurrencies.[7] A parallel set of developments, without regulatory intervention is already on the wheels in India. The world's leading cryptocurrency exchange, Coinbase, announced[8] its plans to establish presence in India. Another powerhouse, Binance, has been in India since 2019 when it acquired the country's largest crypto exchange, WazirX[9]. India is also the second-largest source of web traffic to Paxful,[10] a peer-to-peer bitcoin trading platform, after the United States. While the public seems to be gung-ho about cryptocurrencies in India, the government is in a mind to ban them. It seems that the government is frightened of the consequences of a privately managed settlement system and wants to float its own digital currency to exercise control over the system. In this case, the government is not against the digital currency ecosystem itself, but it is only on the point of 'command and control' intervention. The overall approach to regulating emerging technologies has been a command-and-control type of regulation.

A rule-based, command and control approach has it its own set of issues because it: a) multiplies government control and power – in that it allows for the government decision making itself to become a 'black box'[11]; b) stifles innovation by placing enormous regulatory burden on firms because these approaches also push a regime of excessive compliance. The most important drawback for these kinds of command-and-control approaches also stems from the fact that governments tend to assume digital technologies as no different from traditional technologies. Digital technologies are built on algorithmic frameworks, and algorithms have evolved traditionally predictability models to sophisticated unpredictability representations. The nature of algorithms today themselves can lead to many kinds of harms outside the 'known, visible' harms such as data breach, privacy and security issues, online harms and pricing harms. In enforcing a command-and-control type regulation, the government reinforces the view that it is trying to regulate a space where the pace of transformation is dynamic, but the nature of the technologies is fully comprehensible. This is not true given the unpredictability issues that accompany algorithms.

---

[7] Ministry of Finance. 2019. "Report of the Committee to propose specific actions to be taken in relation to virtual currencies". https://dea.gov.in/sites/default/files/Approved%20and%20Signed%20Report%20and%20Bill%20of%20IMC%20on%20VCs%2028%20Feb%202019.pdf

[8] Crawley, J. 2021. "Coinbase to open India branch". Coindesk. Retrieved from https://www.coindesk.com/coinbase-announces-new-presence-in-india-even-as-potential-ban-on-crypto-looms

[9] Palmer, D. 2019. Binance enters Indian market with acquisition of WazirX. Coindesk. Retrieved from https://www.coindesk.com/binance-enters-indian-market-with-acquisition-of-crypto-exchange-wazirx

[10] To check the statistics at Similarweb, refer https://www.similarweb.com/website/paxful.com/#overview

[11] Frank Pasquale: 'a system whose workings are mysterious, we can observe its inputs and outputs, but we cannot tell how one becomes the other or its use or consequences'. See Pasquele, F. 2015. "The Black Box Society: The Secret Algorithms that Control money and Information". *Harvard University Press.*

Second, India's approach to emerging technologies have always been knee-jerk. Regulations saunter in all of a sudden, as a response to deepening public interest in a new technology.[12] These kind of 'response regulations' can be problematic for a healthy development of an ecosystem where innovation and purpose find instrumental value through rules and guidelines. While there is an immediate need to pass legislations or prescribe guidelines to regulate these emerging technologies, there also remains a deep vacuum in regulatory thinking. These vacuums are temporarily filled through regulatory approaches that do not further the innovation ecosystem while also not delivering effective and efficient public value and purpose. India's regulations are merely need-based. A case in point is India's competition regulator really keen to regulating big digital platforms in India. Every notice that the Competition regulator, Competition Commission of India, has served against a technology platform is a response to some upgrade from the platform on its products and services. These platforms have been gathering mainstream monopoly powers for many years now, but the country's regulatory authorities have investigated complaints and served orders without proactively thinking about regulatory architectures to deal with the challenges posed by emerging technologies.

Third, Indian regulators neither seek to understand the technologies they regulate, nor do they adequately pay attention to public needs such as privacy, algorithmic harms, legal liabilities and democratic values. They are more 'state-focussed' than 'public-focussed', by this we mean that regulators seek to further and enhance state interests as opposed to furthering public innovation and purpose. For example, do Indian regulators take user privacy seriously? From internet activists to lawmakers, this is a question that is in the vanguard of regulating technologies. Can the core principles behind traditional concepts of privacy - like the right to be left alone, the right to have a private life, or to have confidential communications - hold their heft with advancements in technology? While privacy is a constitutionally protected right in India, we do not yet have legal safeguards against misuse of personal data. What the country has is a longstanding Personal Data Protection bill tabled in the Lok Sabha, which is yet to be notified as law. There are grave repercussions to framing new regulations to govern technologies without ensuring that user data is adequately protected. Personal data is collected, used, processed, analysed, shared, transferred, copied,

[12] See Section 2 on Drones

and stored by companies at an extraordinary speed and volume than ever before. Data dominance is one of the key drivers to monopolisation and abuse of dominance by firms. Similarly, governments are also expanding their data collection capabilities evincing mass surveillance fears. In 2001, Justice Antonin Scalia of the United States Supreme Court in his opinion,[13] on a case of enforcement agencies using advanced technology for surveillance into a suspected marijuana grower's house, commented that, "The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."

Also, there has arguably not been a single complete study on the innovation space in India. Many regulators and regulatory bodies provide conflicting guidelines and regulations, but regulators fail to understand that these regulatory requirements also need to be interconnected. For example, to regulate drones in India, it is not only necessary that the country's drone regulatory authority, the Director General of Civil Aviation ("DGCA") to enforce guidelines but it must be in sync with India's data governance regime because drone use is not merely about allowing for drones to fly in India's sky, but it is also about collection of data by the drones, analysis, processing, and utility of the data that is collected. Regulatory governance for emerging technologies must then have a synchronous approach, many regulatory bodies must first understand the technologies, build consensus amongst themselves and collaborate to produce comprehensive regulations that can guide enforcement of rules as opposed to standalone regulatory bodies providing independent guidelines that come into conflict with existing regulations by other regulators.

A case study on the history and enforcement of drone guidelines can be helpful to understand India's regulatory thinking in the emerging technology space.

2. Regulating drone technology in India

'Drones' usually refer to unmanned aerial vehicles, which may be guided by a remote control, at times by an onboard computer system or artificial intelligence. The idea of unmanned aerial vehicles (UAVs) has existed since the mid 1800s. It is said that Austrians attacked Venice using unmanned balloons filled with explosives, and that was the first instance of using

[13] Kyllo v. United States (99-8508) 533 U.S. 27 (2001). Retrieved from - https://www.law.cornell.edu/supct/html/99-8508.ZO.html.

UAVs.[14] Through the world wars, this idea gradually developed, and in the Gulf War, we saw the use of modern-day drones.[15] Initially drones were used specifically for military purposes, but that changed in 2013 when Amazon announced drones as the future of delivery systems.[16]

Since then, drones have been used for commercial and recreational purposes throughout the world, including in India. After Amazon's announcement, other e-commerce companies in India also pushed for the use of drones for delivery. In fact, in Mumbai, a pizza was delivered using drones.[17] Such incidents alarmed the regulators due to non-existence of any legal framework to regulate the usage of drones in the country. The fear and vulnerabilities of national security also surfaced with the increased unregulated usage of drones. In 2015, the Indian Express reported that an unknown person was seen suspiciously flying a drone very close to the residence of the Indian President and the Parliament House.[18] The person could not be tracked, and a lack of regulation added to the fear of security threat, especially with several deadly terrorist attacks which the country witnessed previously.

Consequently, in October 2014, the DGCA announced a blanket ban on drones in the Indian civil airspace.[19] Concerned about security threats, the regulators stated that, "*UAS has potential for a large number of civil applications. However, its use besides being a safety issue, also poses security threats. The Airspace over cities in India has high density of manned aircraft traffic. Due to lack of regulation, operating procedures/ standards and uncertainty of the technology, UAS poses threat for air collisions and accidents.*"[20] The public notice also declared continuation of the blanket ban until the formulation of regulations. The notice further emphasized on the need for approvals from several agencies including defence, home affairs, besides DGCA, pointing towards a highly regulated space.[21]

---

[14] Crilly, B. R. (2011, June 20). Drones first used in 1848. *The Telegraph*. Retrieved from - https://www.telegraph.co.uk/news/worldnews/northamerica/8586782/Drones-first-used-in-1848.html
[15] *Ibid*.
[16] Wallace, Gregory (2013, December 2). Amazon says drone deliveries are the future. *CNN Business.* Retrieved from - https://money.cnn.com/2013/12/01/technology/amazon-drone-delivery/index.html
[17] BBC News (2014, May 23). *India: Police investigate pizza deliveries by drone*. Retrieved from - https://www.bbc.com/news/blogs-news-from-elsewhere-27537120
[18] The Indian Express (2015, October 18). *Unidentified foreign man spotted using drone near Parliament*. Retrieved from - https://indianexpress.com/article/india/india-news-india/unidentified-foreigner-spotted-using-drone-near-parliament/
[19] India Today (2014, October 13). *Civilian drones banned in India: Report*. Retrieved from - https://www.indiatoday.in/technology/news/story/civilian-drones-banned-in-india-report-222975-2014-10-13
[20] Directorate General of Civil Aviation. (2014). *Use of Unmanned Aerial Vehicle (UAV)/Unmanned Aircraft System (UAS) for Civil Applications* [Public notice]. Retrieved from - https://www.dgca.gov.in:443/digigov-portal/?dynamicPage=dynamicPdf/130577810&mainpublicNotices/0/0/viewAllService
[21] *Ibid*.

2.1 Development of Drone Regulations in India

While civilian drone space in India saw a cessation following the blanket ban, worldwide usage of drones made significant progress in diverse sectors ranging from agriculture, infrastructure, power, e-commerce, media and entertainment, disaster management, healthcare, and so on.

In 2016, a report by Goldman Sachs predicted over 100 billion dollars of spending in the commercial drone sector in the upcoming five years.[22] Some Chinese companies like SZ DJI Technology Co. Ltd. controlled over 70 percent of the commercial and consumer drone market with an estimated revenue of 1 billion dollars.[23] In the US, a report by a non-profit organization predicted creation of 100,000 jobs and economic impact of 82 billion dollars from the commercial drone industry by 2025.[24] Another US consultancy firm estimated the global drone market to be 5.93 billion dollars of worth in 2015 and predicted that it would grow to 26.74 billion dollars by 2023, with a growth rate of nearly 21 percent.[25]

A close look at the drone regulations in several countries make it clear that regulations in those countries favour and facilitate the growth of the drone industry. And, unlike India, most countries across North America and Europe did not have a complete ban on civilian drones. For example - in the US, the Federal Aviation Agency (FAA) allowed the civilian usage of drones with caveats, and licenced commercial usage.[26] In the UK, regulatory authorities allowed civilian drone usage with certain prohibitions like permission to operate in restricted zones (near airports). Similar regulations were also in force in Canada. Many of these countries also integrated technology in its regulatory framework - like China, where the rules stipulate an online-real time supervision system that restricts the flight of drones in specific locations and provides for electronic fencing.[27]

---

[22] Market Watch (2016, March 18). *This is how most of the world's businesses will use drones.* Retrieved from - http://www.marketwatch.com/story/this-is-how-most-of-the-worlds-businesses-will-use-drones-2016-03-1
[23] Srinivasan, S. (2018, January 22). Let's open up the skies for drones. *The Hindu Business Line*. Retrieved from - https://www.thehindubusinessline.com/opinion/lets-open-up-the-skies-for-drones/article7780964.ece
[24] *Ibid*.
[25] MarketResearch.com (2017, December) *UAV Drones - Global Market Outlook (2017-2023)* Retrieved from - https://www.marketresearch.com/Stratistics-Market-Research-Consulting-v4058/UAV-Drones-Global-Outlook-11369267/
[26] *Ibid*.
[27] Ananth Padmanabhan (2017, March). *Civilian Drones and India's Regulatory Response*, Carnegie India.

Witnessing the progress worldwide, and increasing domestic demands to relax the rules, the DGCA in April 2016 issued a new set of draft guidelines on the use of UAVs (drones) for civilian or recreational purposes. The draft guidelines categorized drones into 4 categories based on their respective weight, which were - micro, mini, small and large.[28] Issuance of a Unique Identification Number (UIN) by the DGCA was also made mandatory for any kind of operations. This number could only be availed by Indian citizens or companies with principal business in India (which even required the chairman and two-third of the directors of the company to be Indian nationals, and substantial ownership in the hands of Indian nationals); the process for obtaining the number is also elaborate.[29]

Tech-policy researchers argued that the guidelines were flawed, primarily because it did not allow foreign players to operate and would impede technological progress and growth in the drone industry. Also, regulatory gaps existed from concerns of privacy, trespass, other legal liabilities, and ownership of airspace.[30] Public comments were invited on these guidelines by the DGCA for a period of 21 days, and this was followed by a year and half of inaction, with the guidelines never coming into effect.

In November 2017, the DGCA came out with another set of new draft guidelines. Compared to the previous one, the new guideline introduced another category of drones i.e., nano (for drones weighing less than or equal to 250 grams). The new guidelines also proposed operations in visual line of sight, daytime operations and restricted drone usage to 200 feet from the ground.[31] It also introduced the concept of restricted areas for drone operations which include areas within 5 kms from an airport, 50 kms around international borders and beyond 500 metres into the sea. It specifically mentions 5 kms around Vijay Chowk in New Delhi as no-fly zone.[32] The public comments on the guidelines were invited and it was supposed to be finalised by the end of December 2017. However, the final regulations were not released even in early 2018.

Although the new draft was welcomed as a positive response on the part of the Government, it still failed to address several policy gaps including issues such as legal liability and import

[28] Government of India, Office of the Director General of Civil Aviation (2016, April). *Air Transport Circular XX of 2016 – Guidelines for obtaining Unique Identification Number (UIN) & Operation of Civil Unmanned Aircraft System (UAS)*. Retrieved from - http://www.dgca.nic.in/misc/draft%20circular/AT_Circular%20-%20Civil_UAS(Draft%20April%202016).pdf
[29] *Ibid*.
[30] Ananth Padmanabhan (2017, March).
[31] Government of India, Office of the Director General of Civil Aviation. (2017, November 2). *Draft Regulation of CAR on Civil Use of Drones* [Press release]. Retrieved from -https://pib.gov.in/newsite/printrelease.aspx?relid=173164
[32] *Ibid*.

controls. The lack of quality control and standardisation of drones manufactured in India or imported pose a number of challenges. First, when it comes to fixing legal liabilities in case of an accident, it would be a complicated task to ascertain if there was a problem with the device or handling or operations due to the non-existence of standardised quality control of drones. Furthermore, absence of such controls also heightens the vulnerability of these drones to hacking. For example - a drone which is imported into India without import controls may easily come in with malicious software and spyware designed for espionage and surveillance of government installations in the country and hence might pose threat to national security. Therefore, these guidelines seemed to be more of a product of necessity than a well-thought-through futuristic plan to regulate drones in the country.

From a close reading of the guideline, it is evident that one of the primary purposes of it was to prevent disturbances to operations of commercial aircrafts. Besides, the regulation also addressed the security concerns which arose due to unregulated flying of drones especially over strategic positions, government buildings and defence installations. However, there remained several unaddressed policy gaps including - absence of import standardisation and quality control of drones, non-existence of protocol in case of accidents, and the issues of privacy and trespass.

2.2 Drone regulations and guidelines in India

The beginning of 2018 was marked by the formation of groups like the Drone Federation of India, which consisted of stakeholders like companies and start-ups working on the drone sector. Their primary objective was to provide the industry perspective to the Government. Following several consultations with the industry and stakeholders, the Government released the final Civil Aviation Rules on Remotely Piloted Aircraft Systems, on 27th August 2018. These new regulations were known as Drone Regulation 1.0 and were to be effective across India from 1st December 2018.

After years of blanket ban and a series of draft guidelines, Drone Regulation 1.0 was the first concrete step by the Government to regulate drones in the country. There was also a shift in the term used to denote drones - from unmanned aerial vehicles to remotely piloted aircraft systems.

These regulations were issued under the provisions of Rule 15A and Rule 133A of the Aircraft Rules, 1937 and mandated requirements for obtaining Unique Identification Number (UIN), Unmanned Aircraft Operator Permit (UAOP) and other operational requirements like written permission from local police officers. For enforcement it had strong penal provisions and breach of compliance would attract penal action and imposition of penalties under Sections - 287, 336, 337, 338 or any relevant provision of the Indian Penal Code, 1860. In furtherance to that, even provisions of Aircraft Act 1934 and Aircraft Rules 1937 were also to be applied (for non-compliance), many of which prescribe strict actions like imprisonment and hefty penalties.

Evidently the regulations were harsh. The concept of "no permission, no take off" was brought in, but through an enabling regulatory technology solution called - Digital Sky. This platform above all introduced the convenience of filing paperwork for UIN and operator's permit. From a commercial perspective, the Visual Line of Sight (VLOS) conditions which were introduced were restrictive in nature as it discouraged delivery of goods and services using drones. Also, night operations were disallowed and operations to a maximum extent of 400 feet was allowed. While, on the privacy front detailed and clear guidelines never found a place in these regulations except for a provision which stated - "*RPA operator/ remote pilot shall be liable to ensure that privacy norms of any entity are not compromised in any manner.*"[33]

During the release of Regulation 1.0, the Minister of State for Civil Aviation also hinted on a newer and more progressive Regulation 2.0 to address the issues of[34] -

- Certification of safe and controlled operation of drone hardware and software,
- Air space management through automated operations linked into overall airspace management framework,
- Beyond visual-line-of-sight operations,
- Contribution to establishing global standards,
- Suggestions for modifications of existing CARs and/or new CARs.

[33] Government of India, Office of the Director General of Civil Aviation. (2018, December). *Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS)*. Retrieved from - https://www.dgca.gov.in/digigov-portal/jsp/dgca/homePage/viewPDF.jsp?page=InventoryList/headerblock/drones/D3X-X1.pdf

[34] Government of India, Office of the Director General of Civil Aviation (2018, August 27). *Drone Regulation 1.0*. Retrieved from - https://pib.gov.in/newsite/PrintRelease.aspx?relid=183093

During the peak of Covid pandemic in 2020, there was a significant rise in the use of drones by authorities and also several private entities. Government authorities used it for law-and-order enforcement, imposition of lockdown and surveillance for breach of lockdown restrictions, and Covid-19 relief measures.

Realising the effectiveness of drone technology from providing medical relief to remote regions, spraying disinfectants in congested areas to monitoring crowd and lockdown violations, the Government introduced the GARUD portal. Unlike previously when even for Government usage of drones (including relief operations) required to go through the permission process, the new portal allowed for fast-track clearance of exemption requests which came from Government entities.[35]

The silver lining to the pandemic from a technology policy point of view was that it made the regulators realise the importance and need for drones especially in difficult situations. There was also push from the industries for commercial usage of drones. The Federation of Indian Chambers of Commerce and Industry (FICCI) also urged the government to put a blanket ban on the cumbersome permission process for drones during the pandemic, particularly those drones involved in law enforcement, relief operations and critical industries.[36]

Evaluating the situation, the Ministry of Civil Aviation in June 2020 released the draft Unmanned Aircraft System Rules, 2020. These draft regulations were noticeably more detailed and proposed several need-based changes to the existing regulations. First, three new categorizations of drones were introduced namely[37] - remotely piloted aircraft system, model remotely piloted aircraft system and autonomous unmanned aircraft system, apart from the existing weight-based classification from nano to large.

In order to regulate the entire drone ecosystem, the draft rules introduced the concept of authorised person, who can be an importer, manufacturer, trader, owner or operator, who on fulfilment of certain requirements were eligible to obtain authorisation number from DGCA

[35] DGCA launches "GARUD" portal to fast-track exemptions of coronavirus-related drone operations. (2020, May 5) *Business Today*. Retrieved from - https://www.businesstoday.in/current/economy-politics/dgca-launches-garud-portal-to-fast-track-exemptions-of-coronavirus-related-drone-operations/story/402956.html

[36] Coronavirus lockdown: Remove restrictions on drone use for essential industries, govt agencies, says FICCI. (2020, May 4). *Business Today*. Retrieved from - https://www.businesstoday.in/current/economy-politics/coronavirus-lockdown-remove-restrictions-on-drone-use-for-essential-industries-govt-agencies-says-ficci/story/402777.html

[37] Government of India, Ministry of Civil Aviation (2020, June). *The Unmanned Aircraft System Rules*. Retrieved from - https://www.civilaviation.gov.in/sites/default/files/Draft_UAS_Rules_2020.pdf

(valid till a maximum period of five years). Importance has also been given to the quality of drones with both importer and manufacturer requiring a 'certificate of manufacture' from DGCA. Only authorised UAS manufacturers can manufacture in India and can sell or lease only to an authorised UAS trader or authorised UAS owner.

For the first time the idea of having drone ports, drone corridors and a dedicated unmanned aircraft system traffic management in Indian airspace was introduced. Enforcement powers of the regulators and even stricter penal provisions were proposed. Issues like privacy, like previously, remained least deliberated.

In March 2021, the Government released the latest drone regulations - the Unmanned Aircraft System Rules 2021. Shifting from its previous position of territorial applicability, the new rules apply to all drones registered in India. The categorisation and classification of UAS has been based on the draft rules of 2020, but with the introduction of umbrella terms like aeroplane, rotorcraft and hybrid unmanned aircraft system. The new rules have not seen any progress from the draft rules of 2020, the issues of limitations on foreign companies and operators, complicated and rigorous licencing process, detailed framework on privacy and other legal liabilities still remain. Penal and enforcement provisions have been made severe and as well as detailed, prescribing fines for each type of non-compliance.

It would be very early to comment in detail on the new guidelines (which was published towards the end of our work on this paper) as there needs to be further discussions and deliberations around it between the industry and the regulators, but from a first glance, not much progress can be seen from the draft rules of 2020.

2.3 Drone regulations: Challenges to regulatory architecture

Notwithstanding the lack of explicit mention of right to privacy in the Indian Constitution, Indian courts in several cases have recognised the right to privacy. The focus of these judgements was on privacy in the context of harms caused due to violation of privacy. However, the Justice KS Puttaswamy v. Union of India[38] case changed everything. A nine-judge bench of the Supreme Court of India held unanimously that the right to privacy was a

[38] (2017) 10 SCC 641

constitutionally protected right in India, as well as being incidental to other freedoms guaranteed by the Indian Constitution.[39]

Privacy issues relating to drones is self-explanatory. Drones are equipped with high-quality cameras to track their way, but the same cameras can record videos, images and even voice (with an additional microphone) from any point or location by the drone operator. From voyeurs to militants, anyone could use them. Even law enforcement agencies have used drones from time to time for surveillance, silently monitor crowds, manage protests, sometimes even allegedly fitted with facial recognition systems. In India during the protests against the Citizenship Amendment Act and more recently the Farmer's Protest, the law enforcement agencies have used drones for mass surveillance and monitoring. Many of the drones especially in Delhi allegedly used facial recognition software in their drones.[40]

Besides privacy, several other concerns also remain in the drone ecosystem, one of which is the question of property and trespass as drones fly at low altitudes over people's houses and private properties without prior permission from the owners.

Drone-like technologies are a one-way street. Unlike traditional consent infrastructures, an individual neither has any control over the operation of these devices, nor has a say in their deployment. Also, there is very limited user education with regards to these devices. Privacy harms can exponentially multiply without a sound data protection framework. From development to deployment to data collection and monitoring, it is crucial that regulations support embedding privacy as a default feature in every step of the drone architecture. Businesses and governments must also educate users about drones, and reasons for their deployment.

Drones have helped solve some extraordinary problems delivering immense public value. In 1999 during the Kargil War the usage of unmanned aerial vehicles by the Indian army was its first known use in the country. Since then, drone usage has come a long way with exponential growth during the Covid-19 pandemic and the lockdown following it.

---

[39] *Ibid*.
[40] Mandavia, M. (2019, December 31). Activists rally against 'illegal' surveillance of CAA protests. *The Economic Times*. Retrieved from - https://economictimes.indiatimes.com/news/politics-and-nation/activists-rally-against-illegal-surveillance-of-caa-protests/articleshow/73039535.cms?from=mdr

During disaster relief operations, drones have played a crucial role in India. The National Disaster Management Authority, India's top body for disaster management used drones for the first-time during Uttarakhand floods in 2013. Subsequently, drones were used for several relief operations from time to time including floods in Chennai, in Kerala, Bihar and most recently in the Chamoli disaster of Uttarakhand. Besides relief, drones are being used in infrastructure projects be it - roadways, railways, power transmission, pipelines and so on. Even in the agricultural sector, drones are being used frequently. The largest locust swarm outbreak which threatened the nation early last year was also tackled with drones.

During the lockdown following the Covid-19 outbreak, drones were used for spraying disinfectants and enforcement of restrictions on people's movement. States like Uttarakhand and Maharashtra also did trial runs on vaccine delivery.[41] In a topographically diverse country like India, drones seemed like the best possible solution delivery of medical supplies including vaccines.

3. Some recommendations to regulate emerging technologies

The existing drone regulations in the country has been a major roadblock in utilisation of drone capabilities. This is primarily because of the excessive compliance the regulations have brought about from time to time. Besides excessive compliance, regulations have failed to address many of the long-standing issues of privacy and trespass in a detailed manner. The discouragement to foreign players in the drone industry is also a step-backward from global technological advancement. What India needs now is a new set of regulations, addressing several long-standing issues.

How we use and regulate new technologies must be compliant with the spirit of democracy. The current drone regulations fall short of addressing remedies to privacy harms; there is an immediate need to review these regulations to implement privacy-by-design practices including data minimisation and transparency requirements in the current regulatory architecture.

[41] Chakravarty, A., & Rajkhowa, A. (2020, December 17). Drones can make Covid vaccine delivery a success — if Modi govt can just tweak its policy. *ThePrint*. Retrieved from - https://theprint.in/opinion/drones-can-make-covid-vaccine-delivery-a-success-if-modi-govt-can-just-tweak-its-policy/566064/

Another lesser known but important regulatory requirement to investigate into emerging technologies is state capacity. KP Krishnan and Anirudh Burman, in their study on Indian regulators[42], show that the internal motivation to improve regulatory processes within specific authorities is weak in India and this observation applies for emerging technologies as well. India lacks a sound regulatory structure to regulate emerging technologies. The Supreme Court of India observed in a verdict that the absence of a technically competent leadership can weaken good governance[43]. To regulate new technologies, it is mandatory to require an understanding of the mechanisations and technical details of these systems to conduct informed investigations and strengthen regulatory capacity. To understand complex and multifaceted harms such as ones caused by algorithms, it is essential to build skillsets to understand the landscape that emerging technologies operate in. For example, if the competition regulator wants to investigate into a big tech platform, what technical capacities does it need? To investigate into a company's data sharing practices, the regulator needs to understand the technical design of digital systems. We do not yet have an insight into any of India's regulators' institutional capacity.[44] Do they have technically competent bureaucrats to tackle such cases? Do they recruit AI-experts and engineers to understand big tech algorithms? These discussions never feature in any of announcements made by regulatory bodies either.

India's regulators have reached a critical point where they need to build institutional infrastructure to a) carry out algorithmic impact assessments b) develop tools to setup oversight mechanisms and c) establish rigorous standards for compliance. Regulators in India will require significant training to undertake rigorous technical inspections, but this thinking on skillset capacity is lacking in the proposed policies, legislations and regulations. Without building capabilities and competencies, and without understanding the nature of the beast that the regulators are dealing with, how can a fair response be summoned to regulate emerging technologies? Even self-regulation rules in India do not have guidelines to encourage firms to document the technical, product and market scopes of their technology systems or explain their AI systems through explainable AI requirements. Regulators also need to implement monitoring and accountability mechanisms in its regulatory framework. These can include regulatory sandboxes, compliance reports from firms and impact assessment frameworks to

[42] Krishnan, K.P., Burman, A. 2019. "Statutory Regulatory Authorities: Evolution and Impact", in *Regulation in India; Design, Capacity and Performance*, Eds. Devesh Kapur, Madhav Khosla. Bloomsburyprofessional
[43] Techi Tagi Tara v Rajendra Bhandari. 2017. SCC Online SC1165
[44] India's public institutions are afflicted by weak state capacity. See Kapur,D., Mehta, P.B., Vaishanav, M. (eds). 2017. "Rethinking Public Institutions in India". *Oxford University Press*.

audit emerging technologies and their overall infrastructure (from product to service delivery). Attentive to this, we need a planned approach to address current capacity gaps. There are three distinct types of gaps we are dealing with here, namely gaps in a) generating new norms or upgrading old ones for regulating assessment; b) implementing these norms through a readjustment of institutional and behavioural practises; c) enforcing failure to comply with such implementation, be it by private or public actors.

The first set of gaps can be addressed by setting up an independent research body that studies the technical infrastructure of new technologies. This research division must audit and monitor firms; work with them to develop a common reporting system and document these technologies. The second and third set of gaps can only be addressed through a combination of enhancing human resource capabilities and novel thinking. Both implementation and enforcement have a strong accountability component too, one that demands intra- and inter-departmental reporting obligations and constant engagement with other stakeholders such as industry bodies and citizen groups. Therefore, adding people to the government machinery addresses only part of the problem. Real capacity enhancement demands processual reforms including revamp of tracking and monitoring processes, better accountability frameworks including placing responsibility for inter-agency coordination and streamlining of existing processes[45].

An approach of self-regulation for emerging technologies works in good faith but private firms focus on maximising profits and if they are dominant players, they can abuse their dominant position by overriding or skirting legislative authority. Also, soft regulatory measures are not fully comprehensive. Regulating emerging technologies must be studied from the lens of human rights and democratic values than from just from the perspective of economic efficiency. This is because emerging technologies are not merely places that facilitate businesses, but they are also public spaces on their own, where issues of equality, surveillance, discrimination, free speech and disinformation actively conflate with other transactional elements. This means that any direction in regulating emerging technologies must be towards strengthening an effective system of rights that include right to property, the right to contract and rights to due legal process[46]. All these omens such as the lack of a

[45] Padmanabhan, A., Sivasubramanian, A. 2020. "Data Governance and AI regulation in India". *Foreign Commonwealth Development Office*.
[46] For a broad range of disciplinary perspectives including law, public administration, applied philosophy, data science, and artificial intelligence, see Yeung,K., & Lodge,M. 2019. "Algorithmic Regulation". *Oxford university Press*.

procedural, clear, community-oriented, transparent and accountable framework portend towards an urgent need for a radical shift in thinking about what kind of regulatory response India needs to invoke to regulate emerging technologies. India needs to locate the spirit in her regulatory decisions by outlining and envisaging regulatory purpose and values before taking the plunge into enforcing mechanisms to audit and regulate this space.

There is a need for co-regulation[47] where regulators work with stakeholders – consumers, firms, suppliers, engineers, lawyers and ethicists – to build consensus on standards. This co-regulation needs to be adaptive, in that it needs to be dynamic, with faster feedback loops. The Competition and Markets Authority of the United Kingdom speaks thus about algorithms, but it is applicable for regulatory approaches in the emerging technology landscape as well: "with clearer standards and guidance, firms may have a stronger incentive to take steps to design and build transparency and accountability processes into their algorithmic systems, instead of leaving them as afterthoughts instead of a command-and-control approach". This adaptive, co-regulatory approach is something that the Indian government must study. What is required in the Indian emerging technologies regulatory space are clear lines of accountability, state capacity and an urgent need for knowledge capacity. The digital ecosystem is an ever-changing, evolving space. Regulations must be grounded in standard values that need to serve as guidepost, and this needs to be cocreated through transparency, trust, knowledge and extensive participation. We need more policy and legislative tools, interim remedies to address potentially abusive conducts and new definitions of theories of harms to scrutinise new technologies. Indian regulators have only been reactive thus far. But they need to take an adaptive approach to regulation in order to find the right balance in safeguarding interests of the state, enhance ease of doing business, promote democratic rights and encourage innovation that benefits the universe of emerging technologies.

[47] The European Commission High-Level Expert Group on AI suggests that co-regulatory approaches beyond standards can be developed, such as accreditation schemes and professional codes of ethics. Firms that invest in sound data governance, monitoring and keeping records of the behaviour and decisions of their algorithmic systems are better able to identify and mitigate risks, and to demonstrate compliance when needed.