INTERNET FREEDOM FOUNDATION

PARLIAMENTARIANS' GUIDE TO DIGITAL RIGHTS IN INDIA

LEGISLATIVE BRIEF - BUDGET SESSION 2024

Table of Contents

1. Key insights

1.1. Potential Issues to be taken up in the Budget Session

1.1.1. Challenges and Concerns: Delays, Mystery, and Shortcomings in the Digital Personal Data Protection Rules and Act

The Digital Personal Data Protection ("DPDP") Act was passed without adequate public consultation or due consideration to parliamentary rules and procedure. The Act has several deficiencies, such as weak notice requirements for data sharing, storage or transfer, and allows for processing of data without consent "certain legitimate uses" which are left inadequately defined. In fact, the Act is replete with vague or indefinite provisions and, at many instances, leaves implementation of provisions up to rules that will be notified later. Moreover, media reports around the 21 draft rules under the DPDPA, 2023 suggest that they will be released soon on a 45-day public consultation.[1] Where the Ministry of Electronics and IT ("MeitY") invited feedback and public comments on the 24-page draft DPDP Bill, 2022 for 30 days, a 45-day consultation period for 21 draft rules that will give the parent legislation substantive and procedural teeth is highly inadequate and requires reconsideration.[2]

1.1.2. Presidential Approval Grants Official Status to Criminal Reform Laws as Acts of Parliament

Three bills overhauling current Indian criminal laws were passed by both houses of the Parliament in the 2023 Winter Session, and received Presidential assent on December 25, 2023. The bills contain several provisions that threaten the fundamental rights to privacy and free speech. Provisions of the bill attempt to digitise many aspects of criminal procedure, and include 'digital evidence' under the ambit of the evidence law, without outlining procedural safeguards. Though the word 'sedition' has been deleted from the law, the concept is retained through vague provisions, which leaves room for arbitrary application. Executive powers pertaining to search and seizure of digital evidence have also been broadened. The review and recommendations of the Parliamentary Committee on Home Affairs on the bills did not adequately address these shortcomings.

1.1.3. Preserving Colonial Perspectives: Analysis of the Telecommunication Act's Retention of Antiquated Approaches

The draft Indian Telecommunication Bill ("Telecom Bill"), 2023 was passed in the 2023 Winter Session within three days of introduction after minimal discussion. The Telecommunications Act, 2023 echoes the language and choices employed in the colonial Telegraph Act, 1885 and empowers the government to pause transmission and intercept messages "during public

[1]Aditi Agarwal,Draft rules under privacy law almost ready: IT minister, Hindustan Times, October 28, 2023. https://www.hindustantimes.com/india-news/draft-rules-under-privacy-law-almost-ready-it-minister-101698431489684.html.
[2] Public notice for the consultation on the draft 'Digital Personal Data Protection Bill, 2022', Ministry of Electronics and Information Technology, November 18, 2022. https://drive.google.com/file/d/1TmwiMv_MSpZnkk-XljdJeln5f4WZcNPc/view.

emergencies to prevent incitement for committing offenses." This particular measure provides officials with significant authority to monitor and manage messages across the entire telecom network on the broad grounds of public safety. There is also uncertainty regarding the applicability of the Act to “Over-the-Top” (“OTT”) communication services like WhatsApp. The Act allows for excessive surveillance and suspension of internet services without adequate accountability, oversight, or necessary procedural safeguards. It misses a huge opportunity to reform the telecommunication sector and create a rights-centric law that protects user rights instead of infringing on it.

1.1.4. The draft Broadcasting Services (Regulation) Bill, 2023 raises concerns for online free speech

The Ministry of Information and Broadcasting (“MIB”) released the Broadcasting Services (Regulation) Bill, 2023 (“Broadcasting Bill”) for public consultation on November 10 and accepted comments till January 15, 2024. The draft bill includes “Over-the-Top” (“OTT”) content & digital news published by individuals under the regulatory ambit raising concerns for online free speech and journalistic freedom. Exerting executive control over “OTT” content will lead to over-compliance and self-censorship on part of platforms, who will be keen to avoid the wide discretion allowed to the government when it comes to punishments. Risks around censorship of speech expressing satire, irony, sarcasm, dissent, anger, even maybe portrayals of facts and hard-hitting truth which is unpalatable to the Union government or politically influential and powerful communities, may become formalised if the Broadcasting Bill becomes a law of parliament.

1.1.5. Rushed intervention for tackling the issue of Deepfakes must be revisited

In December 2023, MeitY issued an advisory to all intermediaries urging them to follow the due diligence obligations listed under the notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 (IT Rules, 2023).[3] This formal advisory as well as several other notices sent to intermediaries reiterated the need to take proactive steps to curb ‘online harms’ on the internet, particularly the rising instances of deepfakes.[4] In early January 2024, reports surfaced that MeitY is considering amending the IT Rules, 2021 to explicitly define deepfakes and mandate intermediaries to make "reasonable efforts" to avoid hosting them. The media coverage of informal statements by Ministers and unnamed officials around the approach to tackle deepfakes has generated confusion and raised concerns about hasty and superficial interventions. Pursuing rushed policy or

[3]Ministry of Electronics and Information Technology, “MeitY issues advisory to all intermediaries to comply with existing IT rules.”, Press Information Bureau, December 26, 2023. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1990542.
See also: Ministry of Electronics and Information Technology, Gazette notification on the IT Amendment Rules, 2023, April 06, 2023. https://www.meity.gov.in/writereaddata/files/244980-Gazette%20Notification%20for%20IT%20Amendment%20Rules%2C%202023-%20relating%20to%20online%20gaming%20%26%20false%20information%20about%20Govt.%20business.pdf.
[4] “Deepfake menace: Govt issues advisory to social media platforms to comply with IT rules”, The Economic Times, December 27, 2023.
https://economictimes.indiatimes.com/tech/technology/deepfake-menace-govt-issues-advisory-to-intermediaries-to-comply-with-existing-it-rules/articleshow/106297813.cms.

regulatory actions based on a few closed-door meetings with technology platforms without engaging in a broader multi-stakeholder consultation may become counter-productive.

2. Summary of the 2023-2024 Union Budget

2.1. Overall Analysis

The Budget for the Financial Year 2023-2024 was presented in the 2023 Budget Session. Union Budget for Financial Year 2023-24 increased as compared to the 2022-2023 and cumulatively allotted ₹ 1.25 lakh crores to MeitY, MIB, DoT, and Ministry of Home Affairs ("MHA").[5]

2.2. MeitY

The allocation in Budget Estimates (BE) 2023-2024 (₹ 16549 crores) saw an increase of 41.20% as compared to the Revised Estimates (RE) of 2022-23 (₹ 11720 crores), MeitY witnessing the highest increase of 41.2%. However, fund allocation towards PMGDISHA, which is a rural digital literacy scheme, has been completely discontinued. Allocation towards the Digital India Program witnessed a massive decrease of 55.08% and 36.93% in comparison to the allocation made in 2022-2023 BE and RE respectively.

2.3. MHA

The allocation in BE 2023-2024 (₹ 5901.31 crores) saw an increase of 7.83% as compared to the RE of 2022-23 (₹ 5472.44 crores). There has been a marginal hike in the allocation, with the majority of the funds getting directed towards NATGRID, cyber crime, immigration tracking and border management. It is saddening to note a decreasing trend in the budget allocation for Cyber Crime Prevention against Women and Children and Miscellaneous Schemes.

2.4. MIB

The allocation in Budget Estimates (BE) 2023-2024 (₹ 4692 crores) saw an increase of 12.19% as compared to the Revised Estimates (RE) of 2022-23 (₹ 4182 crores). However, this increase must be perceived with a note of caution as the capital budgetary allocation has decreased by 10.86% as compared to the previous revised budget. This reflects poorly on the MIB's planned spending for the current financial year as the majority of its budget increase is targeted towards revenue expenditure.

2.5. DoT

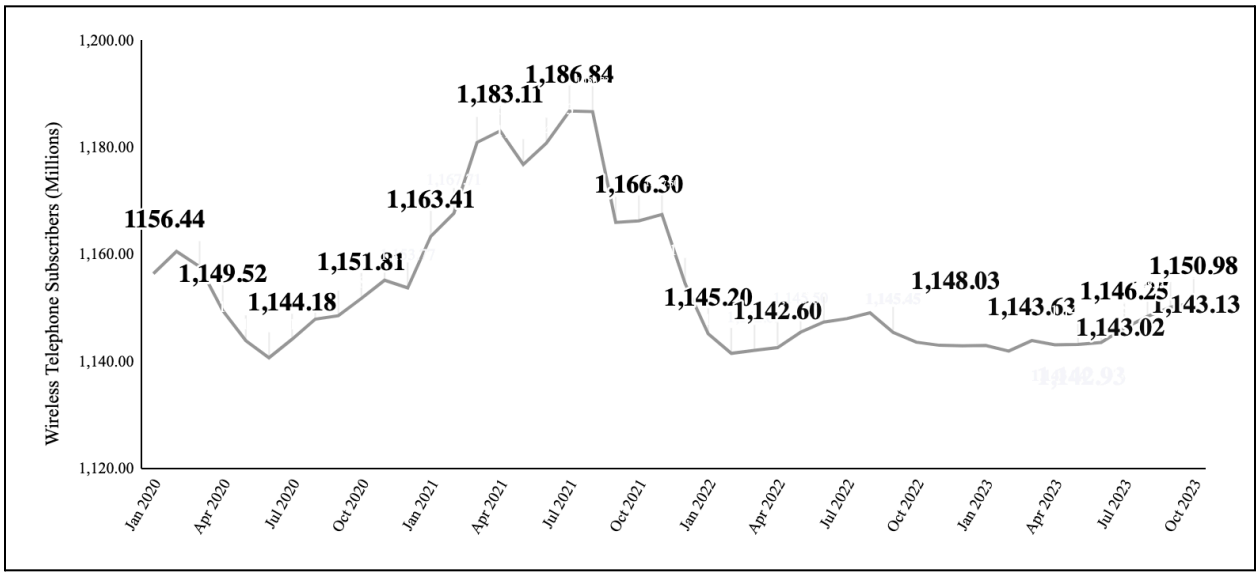
The allocation in Budget Estimates (BE) 2023-2024 (₹ 97579.1 crores) saw an increase of 19.25% as compared to the Revised Estimates (RE) of 2022-23 (₹ 81821.1 crores). An allocation of ₹5.56 crores for 5G Connectivity test bed saw a decrease of 28.16% from RE 2022-23 (₹7.74). As far as allocations for Bharatnet are concerned, there has been a significant increase of 233.33% in BE 2023-24 (₹5000 crores) from RE (₹1500 crores) and a decrease of 28.57% from BE 22-23 (₹7000 crores).

[5] Tejasi Panjiar and Prateek Waghre, "Previously under-utilised budgets make us wary of the increased allocation in the 2023-2024 Budget", Internet Freedom Foundation, February 03, 2023. https://internetfreedom.in/budget-2023-2024/.

3. Key statistics

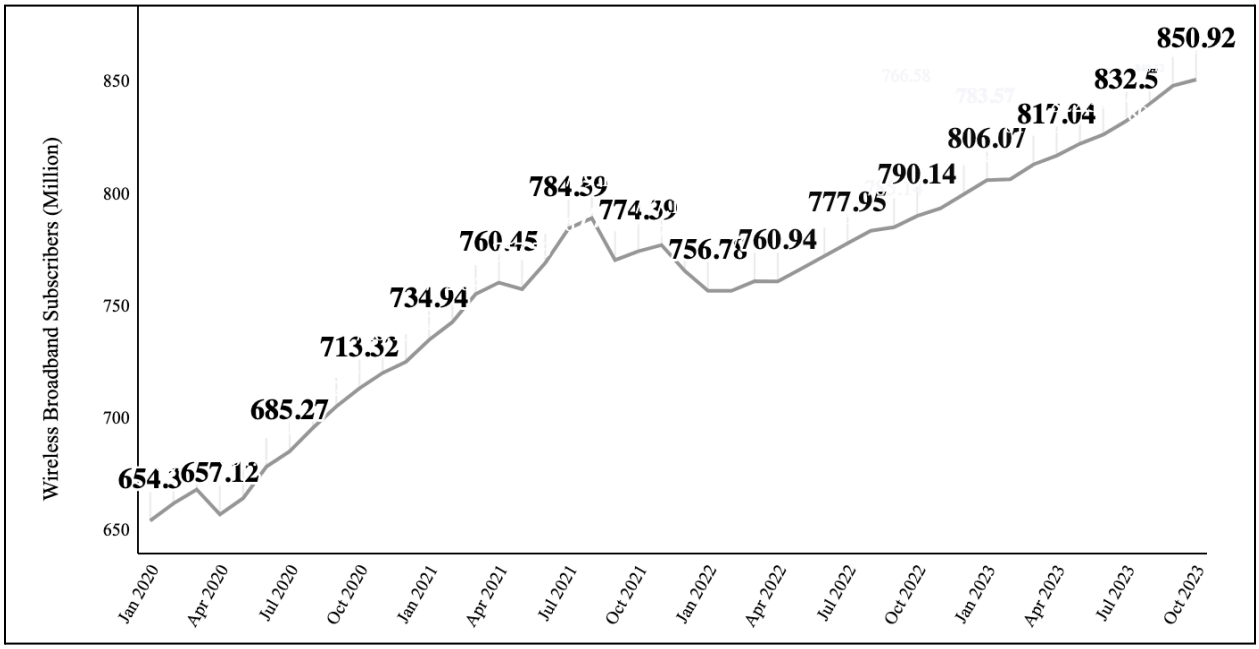
3.1. Connectivity Tracker

Figure 1: Wireless telecom subscribers witnessed an inconsistent rise from June 2020 till August 2021, after which they declined till February 2022. While it saw a gradual rise till August 2022, it registered a dip till December 2022. Following a prolonged stagnation, it has steadily risen since July 2023.



Source: TRAI's Broadband Subscription Reports

Figure 2: Wireless broadband subscribers witnessed steady growth until November 2021. After a dip in February 2022, they have experienced steady growth since then, continuing until October 2023.



Source: TRAI's Broadband Subscription Reports

3.2. Schemes

3.2.1. BharatNet: Delayed Implementation and Unspent Budget Concerns

The phased implementation of the BharatNet project aims to extend broadband last-mile connectivity to all Gram Panchayats (GPs) nationwide. However, the current deployment pace raises concerns. As of November 29 2023, 2,12,081 GPs have been made service-ready according to a Lok Sabha question.[6] However, data.gov.in paints a different picture with just 1,93,472 service ready GPs as of November 30 2023 with no apparent explanation for the delta.[7] In 2023, the government spent only ₹7629 Crore, falling short of the budgeted ₹9,000 crore. This marks the sixth consecutive year of slowed funding for the Universal Service Obligation Fund (USOF), while over ₹77,000 crore remains unutilized from the fund. The telecom body Cellular Operators Association of India (COAI) called for a stop on the mandated contribution of 5% of Adjusted Gross Revenues to the USOF fund until the outstanding balance has been utilised.[8] Despite this, various regions in India continue to be underserved and disconnected. The government plans to infuse ₹ 41,331 crore into the ongoing BharatNet project.[9]

3.2.2. National Broadband Mission: Slow Progress Towards Delayed Target

The primary objective of the National Broadband Mission (NBM), an extension of the BharatNet project, is to enhance digital communications infrastructure and achieve universal and affordable broadband access for all by 2022 - a deadline which has already been extended to 2024-2025.[10] As of May 31, 2023, 7.60 lakh towers have been installed under the NBM, falling short of the planned target of 10 lakh towers. The Ministry of Communications (MoC) attributes the sluggish progress of PM-WANI and NBM to challenges such as the "non-availability of suitable locations, transportation difficulties, and various procedural formalities with local administration/agencies for tower installations."

3.2.3. Budget for PMGDISHA discontinued

Initiated in February 2017 to cultivate skills and empower marginalised communities, this program aimed to digitally educate 6 crore individuals by March 31, 2019 and a 1 crore enrollment target was set for FY 2023-24. As of December 31, 2023, only 4.70 crore candidates have received certification with 50 lakh having been certified in the current year.[11] Notably, the Budget for 2023-2024 from MeitY did not allocate any funds to PMGDISHA, breaking the trend

[6] Lok Sabha unstarred question no. 543 on National Broadband Mission. https://sansad.in/getFile/loksabhaquestions/annex/1714/AU543.pdf?source=pqals.
[7] District-wise Service Ready Gram Panchayat Status under BharatNet as on 30-11-2023. https://data.gov.in/resource/district-wise-service-ready-gram-panchayat-status-under-bharatnet-30-11-2023.
[8] Shouvik Das, "Telco body seeks USOF, tax reliefs in FY25 Union Budget", Mint, January 19, 2024. https://www.livemint.com/industry/telecom/telco-body-seeks-usof-tax-reliefs-in-fy25-union-budget-11705603610343.html.
[9] Lok Sabha unstarred question no. 1695 on USOF. https://sansad.in/getFile/loksabhaquestions/annex/1714/AU1695.pdf?source=pqals.
[10] Lok Sabha Unstarred Question No. 2183 on National Broadband Mission. https://sansad.in/getFile/loksabhaquestions/annex/1712/AU2183.pdf?source=pqals.
[11] "Monthly Achievements for the month of December, 2023", Ministry of Electronics and Information Technology, https://www.meity.gov.in/writereaddata/files/Monthly%20Achievements%20MeitY%20December%202023.pdf.
See also: "Outcome budget 2023-2024", Ministry of Finance, https://www.indiabudget.gov.in/doc/OutcomeBudgetE2023_2024.pdf.

of continuous budgetary support for the rural digital literacy scheme since its inception in 2017.

3.2.4. PM-WANI Hangs in the Balance

Prime Minister Wi-Fi Access Network Interface (PM-WANI) was launched in December 2020 in order to empower local businesses or Public Data Offices (PDOs) to set-up WiFi hotspots and access points to democratise access and generate employment.[12] ISPs are charging exorbitant prices for leased line internet access to PDOs and PDO Aggregators - up to 8 Lakh a year for a single internet-leased line. Initially, Public Data Offices (PDOs) had to pay 8% of their gross revenue to the DoT as an operating fee which has now been nullified with an intent to increase investment in the scheme. While the DoT has written to the TRAI reiterating the need for a reduction in leased line charges for small businesses, TRAI refuses to take action against ISPs.[13] With only 1,48,00 public hotspots and a target of 5,00,000 by 2030, the scheme's future hangs in the balance.[14] The number of Wi-Fi Hotspots deployed under the PM-WANI scheme in 2022 were 1,34,904, which indicates severely stagnated progress which is further exacerbated by no increase in the budget from FY 2022 to combat low adoption numbers.[15]

[12] Tarun Pratap, "PM WANI: The PCO model of Public Wi-Fi stands to fulfill long pipe dream", Digital Empowerment Foundation, 2021. https://www.defindia.org/wp-content/uploads/2021/03/PM-WANI-Report_23-March-2021.pdf.
[13] Jatin Grover, DoT, "Trai spar over PM Wani programme", Financial Express, October 6, 2023. https://www.financialexpress.com/business/industry-dot-trai-spar-over-pm-wani-programme-3264281/.
[14] Aditya Sinha and Paras Ratna, "Digital Public Goods and India's Diplomatic Outreach in the Indo-Pacific", Institute for Competitiveness and US Asia Technology Management Center. https://www.competitiveness.in/wp-content/uploads/2023/11/TID_WP_10_DPGs_Sinha_and_Ratna.pdf.
[15] Standing Committee On Communications And Information Technology (2022-23), "Demands For Grants (2023-24) Forty-Third Report", Ministry Of Communications (Department Of Telecommunications), March 2023. https://loksabhadocs.nic.in/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_43.pdf

4. Key areas of Digital Governance

4.1. Privacy and Data Protection

4.1.1. Digital Personal Data Protection Act (DPDPA), 2023 disappoints with inadequate provisions and delays in the release of its rules

In light of some reporting around the finalisation of the 21 draft rules under the DPDPA, 2023 and its imminent release, the Ministry must reconsider the reported 45-day timeframe for inviting public comments.[16] Although several reports indicated that the rules under the DPDPA, 2023 will be released for public consultation in early January, these timelines have not been adhered with, leading to uncertainty.[17] Several stakeholders, including civil society, have raised concerns with provisions of the Act, some of which are listed below.[18]

Concerns:

- The Act excludes from its ambit any publicly available personal data, which makes data principles vulnerable to online scraping.
- It has weak notice requirements for data sharing, storage or transfer, and worryingly imposes duties and penalties on data principles.
- The Act is replete with vague or indefinite provisions – processing of data without consent is allowed for "*certain legitimate uses*" which is not adequately defined.
- Cross-border data transfer provisions are vague and only extend to countries not specified in a 'blocklist' which is to be notified later.
- In many instances in the Act, enforcement is left up to rules that will be notified later by the Union Government.
- Additionally, sweeping exemptions may be awarded to the Union Government and private actors, through rules.
- The right to information has been diluted.
- The Act fails to provide safeguards against overbroad surveillance.
- The Data Protection Board, a statutory body slated to oversee the implementation of the Act, may not be an independent, neutral and impartial body, and is empowered to direct the Union Government to block access to information in public interest.

4.1.2. Foundational Principles for the Upcoming Digital India Act

The Digital India Bill is yet to be released in the public domain, which aims to overhaul the two-decade old, current legal framework governing the rapidly changing digital ecosystem,

[16]Aditi Agarwal,Draft rules under privacy law almost ready: IT minister, Hindustan Times, October 28, 2023. https://www.hindustantimes.com/india-news/draft-rules-under-privacy-law-almost-ready-it-minister-101698431489684.html.
[17] "Govt to notify rules for DPDP Act by January end, says Rajeev Chandrasekhar", Money Control, December 06, 2023. https://www.moneycontrol.com/news/technology/govt-to-notify-rules-for-dpdp-act-by-january-end-says-rajeev-chandrasekhar-11861991.html.
[18]Anushka Jain & Prateek Waghre, "IFF's first read of the draft Digital Personal Data Protection Bill, 2023", IFF, August 03, 2023, https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2023/.

i.e. the IT Act, 2000. The "Digital India Act" ("DIA") has been a subject of great discussion and speculation in the last few months, but has not been released for public consultation yet.

Concerns:

- There is a need for a truly open and public consultation process before bringing in a law such as the "DIA" that would affect ordinary Indians.
- Before replacing the IT Act, 2000, its existing lacunae and inadequacies must be studied and resolved so that the new law does not replicate them.

Recommendations:

- MeitY may collaborate with multiple and diverse stakeholders and work towards building a statutory framework that safeguards the user through an open, transparent and deliberate public consultation.
- MeitY may publish a white paper underlining its intent with the "DIA" and conduct broad-based stakeholder consultations around it before such a law is brought to the parliament.
- Such a white paper or discussion paper should include, but not be limited to, a clear articulation of the issues, risks or harms considered by the government, the results and analysis of any cost-benefit analysis undertaken by the government, the options or alternatives considered by the government to deal with these issues and their position on each of them, and so on.
- Further, the new digital legal framework should be based on constitutional principles, enshrining constitutionally guaranteed fundamental rights.

4.1.3. Surge in data breaches

In recent times, India has faced a surge in cyber attacks and security threats targeting both public and private databases:

- In early October 2023, it was uncovered that the National Logistics Portal exposed sensitive credentials and secret encryption keys through publicly accessible JS files on its website. Furthermore, numerous Amazon Web Services S3 buckets containing personal data such as worker information, marine crew details, invoices, and internal documents were found to be openly accessible to the public.
- Subsequently, on October 31, 2023, a database purporting to contain sensitive personal details of 81.5 Crore Indian citizens, including Aadhaar and passport numbers, was reportedly available for sale on the dark web platform 'BreachForums' since October 9, 2023.
- The state-owned telecom operator Bharat Sanchar Nigam Ltd (BSNL) reportedly suffered a significant data breach.[19] The leaked data reportedly includes sensitive

[19] Dia Rekhi, "BSNL suffers data breach; sensitive info of users up for sale on dark web", The Economic Times, December 22, 2023. https://telecom.economictimes.indiatimes.com/news/industry/bsnl-suffers-data-breach-sensitive-info-of-users-up-for-sale-on-dark-web/106197459.

personal data such as email addresses, billing details, contact numbers, mobile outage records, network details, completed orders, and customer information.

- The System for Pension Administration Raksha (SPARSH) portal, a dedicated government pension portal for defence personnel, allegedly suffered a data breach which resulted in the leak of sensitive information such as usernames, passwords, pension numbers, and more of thousands of defence personnel.[20] In a worrying development, access credentials to this sensitive information emerged on Telegram, posing a risk of potential misuse and manipulation of vital pension-related processes.
- Reportedly, the Madhya Pradesh's e-Nagarpalika portal suffered a cyber attack which corrupted the entire data of 413 cities and towns covered under the portal.[21] The portal oversees welfare service delivery mechanisms such as birth and death as well as marriage certificates, payment of property, water and sanitation taxes, etc.

India has witnessed several high-profile data privacy breaches, including sensitive medical and financial data. More recently, leaks in the servers of Zivame, RentoMojo, CoWIN, and AIIMS have raised concerns about the effectiveness of existing governance mechanisms in response to such breaches. A non-exhaustive list of data breaches in the country since 2020 is available on the publicly accessible database PlugTheBreach, a small-scale initiative by the Internet Freedom Foundation (IFF) to cover, report, and track data breaches in India to enhance transparency and public awareness.

4.1.4. Right to transparency attacked with the recent exception of CERT-In from the RTI Act, 2005

An amendment to the Second Schedule to the Right to Information ("RTI") Act, 2005 was notified by the Department of Personnel and Training (DoPT) on November 24, 2023, exempting the Indian Computer Emergency Response Team (CERT-In) from providing information under the Act.[22] This move is certainly not in the public interest as it weakens the rights of the people by diluting an Act meant to empower them.

Concerns:

- The exclusion of CERT-In from application of the Act, in an environment where data breaches, device vulnerabilities, and deployment of illegal spywares occur frequently, significantly erodes its accountability.

See also: IFF's letter on the BSNL data breach numbered IFF/2023/060, December 27, 2023. https://drive.google.com/file/d/1EkTNIDjS4WwVK6edRVBO22CZsp-tm4dd/view.

[20] Samiksha Jain, "TCE Exclusive: Massive Data Leak at India's SPARSH Pension Portal Puts Defense Personnel at Risk," The Cyber Express, 8 January 2024. https://thecyberexpress.com/sparsh-portal-data-leak-exposes-sensitive-info/.
See also: IFF's letter on the SPARSH data breach numbered IFF/2024/007, January 12, 2024. https://drive.google.com/file/d/1saYziL2X6a9encIgW7t2Rp3jh4Gxi1sg/view.

[21] Press Trust of India, "MP's e-Nagarpalika portal covering 413 urban areas suffers cyber attack, data corrupted", Economic Times Government. December 24, 2023. https://government.economictimes.indiatimes.com/news/secure-india/mps-e-nagarpalika-portal-covering-413-urban-areas-suffers-cyber-attack-data-corrupted/106244138.

[22] https://egazette.gov.in/(S(qfgob4mjixsp5xt2czi5w3s2))/ViewPDF.aspx?ref=static.internetfreedom.in

- This move for an organisation like CERT-In that investigates cyber-security vulnerabilities in public and private infrastructures may undermine the constitutional rights of citizens to their privacy, and to information.

4.1.5. Health Data Concerns with NHA's Ayushman Bharat Mission

Under the Ayushman Bharat Digital Mission ("ABDM"), the National Health Authority ("NHA") stores widespread data of Indian citizens availing various health schemes and services. One such scheme, proclaimed as one of the worlds' largest government-funded health insurance schemes, is the Ayushman Bharat Pradhan Mantri Jan Aaroya Yojana ("AB PM-JAY"). The scheme seeks to promote universal health coverage in India by providing free health services to a bracket of "vulnerable" populations in India and since its launch, has registered over 28 Crore beneficiaries and empanelled over 27,000 hospitals.[23]

Concerns:

- The NHA under ABDM has weak privacy safeguards for the large amount of patient data it collects. Its Health Data Management Policy suffers from many deficiencies including non-specific and irrevocable consent requirements.[24]
- The NHA also potentially publishes and publicly displays the sensitive medical data of up to 28 Crore patient beneficiaries under the AB PM-JAY on its scheme websites, without patient consent and data security principles in place. Sharing personally identifiable information on a public forum is a glaring violation of constitutionally-guaranteed patient privacy and NHA's own Health Data Management Policy which governs the AB PM-JAY. This obligation cannot be overridden through the Digital Personal Data Protection Act, 2023 either.

Recommendations:

- Unless the beneficiaries have specifically consented to NHA publishing their details on its websites, which presumably they have not since the permission is not specifically sought by the NHA, their personal data be taken down and not published on any scheme websites.
- Such high volumes of patient data should not be stored centrally after the conclusion of their treatment, and that patients must be empowered to have control over the storage and sharing of their health data.

4.1.6. Draft Guidelines on Dark Patterns: A Critical Overview

The draft Guidelines for Prevention and Regulation of Dark Patterns were published by the Ministry of Consumer Affairs, Food and Public Distribution for public consultation on September 7, 2023, until October 5, 2023. They set a satisfactory preliminary framework to

[23] NHA Setu Dashboard, https://dashboard.pmjay.gov.in/pmj.
[24] Disha Verma, "AB PM-JAY counts patients but discounts patient privacy," Internet Freedom Foundation, January 04, 2024, https://internetfreedom.in/ab-pm-jay-patient-privacy/.

start monitoring and regulating dark patterns, but there was certainly scope for improvement. On December 1, 2023, the Ministry published a revised set of Guidelines which address such deficiencies.[25]

Concerns:

- Clause 8 from the draft Guidelines, stating "*the provisions of the Act [Consumer Protection Act, 2019] shall apply to any contravention of these guidelines*," has been removed from the revised version for being too vague and overbroad.
- While vague penalty provisions are dangerous, removing them from the draft creates even more uncertainty. Use of dark patterns is 'prohibited' under Clause 4, yet there is no provision prescribing the consequences of contravening the Guidelines. The Consumer Protection Act, 2019 may be employed on a case-by-case basis by the CCPA, but the Guidelines must immediately provide clarity on this front.[26]
- Consumer protection extends to physical spaces as well, where consumer consent and autonomy must be guarded against covert coercion and deceptive marketing by public and private players. Ministry of Civil Aviation's Digi Yatra initiative, which is supposedly an expedited check-in service at airports, is deploying facial recognition technology to scan passengers' faces and their boarding passes without their consent.[27]
- Digi Yatra already raises a number of concerns in relation to data collection, storage, and processing with weak or non-existent privacy safeguards. On top of this, passengers are being coerced into opting for it over a regular airport check-in, through deception and coercion by airport staff.[28]

Recommendations:

- To apply the Guidelines justifiably in the domain and equitably for small and big entities, the Ministry must set clear parameters for penalising dark patterns. Owing to their deceptive nature, it may be tricky to see if a dark pattern was employed by an entity with the intention to deceive – so it might be useful for the Ministry to opt for a case-by-case assessment on merits to establish intent, and penalise the entity accordingly.
- While adjacent practices like misleading advertisements and unfair trade practices are penalised in other laws in force in India, dark patterns are notorious for being more covert and difficult to detect. A misleading advertisement may be easier to identify and report based on its language and features, and therefore easier to regulate, than

[25] "Guidelines for Prevention and Regulation of Dark Patterns, 2023", Ministry of Consumer Affairs, Food and Public Distribution, https://egazette.gov.in/WriteReadData/2023/250339.pdf.
[26] Disha Verma, "Jago online market entities jago! A look at how the revised Dark Patterns Guidelines attempt digital consumer protection", Internet Freedom Foundation, December 06, 2023, https://internetfreedom.in/revised-dark-patterns-guidelines/.
[27] Jagriti Chandra, "Centre's Digi Yatra enrolment takes off as airport security staff sign up flyers without their consent", The Hindu, January 05, 2024, https://www.thehindu.com/news/national/passengers-say-cisf-and-airport-staff-are-collecting-biometric-data-without-consent/article67710134.ece. See also: IFF's compilation of passenger experiences and grievances re: DigiYatra on X (formerly Twitter), https://x.com/internetfreedom/status/1731984956828582172.
[28] Disha Verma, "Resist Surveillance Tech, Reject Digi Yatra", Internet Freedom Foundation, January 16, 2023, https://internetfreedom.in/reject-digiyatra/.

dark patterns in physical spaces. The Ministry must keep up the momentum and expand its mandate to such prevalent but nefarious physical dark patterns as well.

4.1.7. RTI Act Amendment: CERT-In Exemption

The Department of Personnel and Training (DoPT) notified an amendment to the Second Schedule of the RTI Act, 2005 on November 24, 2023, exempting the Indian Computer Emergency Response Team (CERT-In) from disclosing information under the Act. This development is not aligned with the public interest, as it diminishes the people's rights by diluting a law designed to empower them. The exclusion of CERT-In from the Act's application in an environment marked by frequent data breaches, device vulnerabilities, and the deployment of illegal spyware significantly diminishes its accountability. The reported impact of breaches on around 29,20,52,503 Indians from 2004 to the second quarter of 2023, averaging 9904 breaches per 1 lakh people, underscores the importance of maintaining transparency and accountability in this context.

4.2. Platforms governance and censorship

4.2.1. Challenging the constitutional validity of the fact checking provision under IT Amendment Rules, 2023 in the Bombay High Court

The Union Government notified amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Amendment Rules, 2023") On April 06, 2023. The Rules allow for a notified fact check unit, (created solely on the discretion of the Union Government), that will be empowered to identify "fake", "false" or "misleading" online content related to the government. It is worth noting that these amendments, with its wide ranging implications, were notified despite the IT Rules, 2021 not being tabled in the Lok Sabha. This is deeply concerning as the government, as per parliamentary procedure, is required to table the Rules in the Parliament within 15 sitting days of its notification.[29] Since the IT Amendment Rules, 2023 were notified on the last day of the 2023 Budget Session, the Ministry must table the amended rules within 15 days of the date of commencement of the upcoming session.

The Bombay High Court is currently hearing a constitutional challenge to the IT Amendment Rules, 2023 insofar as they enable a government established Fact Check Unit to identify false, fake or misleading information about itself on social media.[30] The matter was last adjourned on January 15, 2024, to be heard next on January 31, 2024.

Concerns:

[29] "Manual of Parliamentary Procedures in the Government of India", Ministry of Parliamentary Affairs, May 2018, https://www.mpa.gov.in/sites/default/files/Manual2018_0_0.pdf.
[30] Tanmay Singh, "Bombay HC reserves its judgment in petitions challenging the Union Government's fact checking amendments, after final hearings conclude", Internet Freedom Foundation, September 29, 2024, https://internetfreedom.in/it-rules-2023-bombay-hc-reserved-judgement/.

- The Amendment would make the Union Government the effective arbitrator of 'free speech' with regards to its own affairs, thus bypassing the principles of natural justice.[31]
- Further, the inclusion of this provision under Rule 3(1)(b)(v) makes taking action against content identified by such a fact check unit a due diligence requirement for intermediaries. In the event they fail to do so, they risk losing their 'safe harbour' status.
- The constitutionality of this provision is currently under challenge in the Bombay High Court in a batch of petitions filed by Association of Indian Magazines, Kunal Kamra and others, arguing that it violates the IT Act, 2000, and infringes on the rights to freedom of speech and expression and the right to practise one's trade and profession.[32] On September 26 and 27, 2023, the Hon'ble Solicitor-General of India, Mr. Tushar Mehta, on behalf of the Union Government, made submissions clarifying that the fact-check unit's primary focus is on identifying patently false government-related content, with its role limited to flagging and providing feedback on misinformation. As per the latest update, the Bombay High Court has reserved its judgement, to be pronounced tentatively on December 1, 2023.[33]

4.2.2. Unchecked blocking and takedown powers of government functionaries

4.2.2.1. Blocking and takedown of content on social media platforms

In January 2024, Twitter/X account of the research group Hindutva Watch was withheld in India in response to a legal demand under Section 69A of the IT Act, 2000.[34] It is unclear whether the due process was followed under Section Section 69A of the IT Act, 2000 and the 2009 Blocking Rules.

Earlier in March 2023, an internet shutdown was put into effect for nearly 27 million people by the Government of Punjab in response to unrest around the arrest of Amritpal Singh. Social media accounts of journalists, activists, and civil society organisations within and outside India were arbitrarily identified and blocked for all four days of the internet shutdown. The reasons for withholding these accounts were not made public, and it remained unclear whether blocking orders were provided to the affected persons, and whether an opportunity to be heard was provided before issuing such blocking orders.

Concerns:

[31]Tejasi Panjiar & Prateek Prateek, "IT Amendment Rules, 2023 are a nightmare, dressed like a fact checking daydream", IFF, April 21, 2023, https://internetfreedom.in/public-brief-it-amendment-rules-2023.
[32]Amisha Shrivastava & Awstika Das, "How Is News Any Less Fake Or Misleading In Print?' Bombay High Court Expresses Concerns About IT Rules Singling Out Digital Content", LiveLaw, July 13, 2023, https://www.livelaw.in/high-court/bombay-high-court/bombay-high-court-fake-news-it-rules-free-speech-singling-out-digital-news-print-media-kunal-kamra-article-19-232671.
[33]Tanmay Singh, "Bombay HC reserves its judgement in petitions challenging the Union Government's fact checking amendments, after final hearings conclude", Internet Freedom Foundation, September 29, 2023, https://internetfreedom.in/it-rules-2023-bombay-hc-reserved-judgement/.
[34] "Indian Government Has X Account of 'Hindutva Watch' Withheld", The Wire, January 17, 2024, https://thewire.in/rights/indian-government-has-x-account-of-hindutva-watch-withheld.

- Arbitrary blocking is harmful not only for operational transparency but also for India's democratic ethos.
- MeitY is empowered to block information only if it is necessary to do so in limited contexts, while adopting transparency in exercising such powers.

Recommendations:

- Blocking orders must be furnished to the affected persons, and made public to ensure transparent and accountable exercise of powers. Such disclosure will not only ensure transparency and fairness, but also foster public trust in the public authorities that are constrained to block websites in accordance with law.

4.2.2.2. Blocking and takedown of applications and online services

In November 2023, MeitY issued blocking orders against 22 illegal betting apps & websites, including Mahadev Book and Reddyannaprestopro, following investigations by the Enforcement Directorate against these apps.[35] On May 1, 2023, it was reported that 14 mobile applications that provided end-to-end encrypted messaging services, enabled peer-to-peer ("P2P") messaging, etc., were banned purportedly on the basis that they were being used by terrorists in Jammu & Kashmir.[36]

Concerns:

- Reasoned blocking orders and a pre-decisional hearing were not provided to these apps. This raises substantial concerns, as it undermines the fairness of the process and denies individuals their right to challenge the exercise of power under Section 69A of the IT Act, 2000.
- The constitutional validity of Section 69A and the Blocking Rules, 2009 was upheld in the *Shreya Singhal v. Union of India* case, with the requirement of a reasoned order and adherence to procedural safeguards, including a hearing.
- Notably, Section 69A is not designed to block entire smartphone applications, as its jurisdiction is limited to individual pieces of information and content.

Recommendations:

- The banning of these apps, several of which provided essential services, such as encrypted or P2P platforms for messaging, sets a very worrying precedent. It not only affects the day-to-day tasks and livelihood of users, but also restricts access to such services for users who rely on them for secure communication. These users may include journalists, activists, whistleblowers.

[35]MeitY, "MEITY issues blocking orders against 22 illegal betting apps & websites, including Mahadev Book Online on request of Enforcement Directorate", Press Information Bureau, November 05, 2023. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1974901.
[36]"Centre bans 14 apps in J&K citing use by terror organisations", The Hindu, May 1 2023, https://www.thehindu.com/news/national/centre-blocks-14-mobile-messenger-apps-being-used-by-terrorist-groups/article66799154.ece.

- Restrictions on freedom of speech and expression must be meticulously tailored and justified based on the enumerated grounds in Article 19(2) of the Constitution. Any restrictions imposed under Article 19(2) must be reasonable and proportionate.[37]

4.3. Denial of rights through Internet Shutdown

India continues to be the country with the most number of internet shutdowns in the world.[38] The Hon'ble Supreme Court in *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 63 and *Foundation of Media Professionals v. Union Territory of Jammu & Kashmir*, (2020) 5 SCC 746 recognised that the right to speech and the right to carry on any trade through the medium of the internet is constitutionally protected.

In an internet shutdown, access to healthcare, education, banking facilities, and livelihood, are all impacted. The economy also suffers drastically. Access to government welfare schemes, which are dependent on the internet, is also impeded. Workers dependent on rural employment guarantee schemes are impacted as well, as they lose wages due to not being able to mark their attendance on a government app due to internet suspension.[39] The only procedural safeguard afforded by the Telecom Suspension Rules against internet shutdowns is in the form of a Review Committee, headed by the State's Chief Secretary, which must meet and determine the legality of the internet shutdown orders.

Concerns:

- Uptil now this year, internet services were suspended at least 44 times in India. Out of which internet services were suspended in Manipur at least 14 times.
- Reports suggest that Jammu and Kashmir witnessed the highest number of internet suspensions in the world.
- November 23, 2023 marked over 200 days of Manipur's ongoing state-wide internet shutdown. The state-wide internet shutdown has been in place since May 3, 2023. Since the second day of the shutdown, all internet services have been suspended through templatized orders issued every five days.
- The Rajasthan government imposed an internet shutdown in several districts of the State to prevent incidences of paper leak during the Rajasthan Public Service Commission (RPSC) examinations on January 7, 2024.[40]
- In 2023, India lost $255.2 million because of shutdowns. India had 2,353 hours of shutdown affecting "43.2 million users in India."

[37]"Mayday Alert: 14 mobile apps banned, no blocking order released. #WhatTheBlock" , IFF, 10 May 2023, https://internetfreedom.in/14-mobile-apps-banned.
[38]Human Rights Watch & IFF, supra.
[39]Human Rights Watch & IFF, ""No Internet Means No Work, No Pay, No Food" Internet Shutdowns Deny Access to Basic Rights in "Digital India"", June 14, 2023, https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic#:~:text=Human%20Rights%20Watch%20and%20Internet%20Freedom%20Foundation%20identified%20127%20shutdowns,once%20in%20these%20three%20years.
[40] Sarasvati NT, "Rajasthan Government Issues Yet Another Internet Ban To Prevent Cheating During Examinations", Medianama, January 08, 2024, https://www.medianama.com/2024/01/223-rajasthan-govt-internet-shutdown-rpsc-exam-cheating/.

- On December 01, 2021, the Standing Committee on Information Technology in its 26th report stated that the Union Government did not collect empirical data to show that the suspension of internet services improved law and order situations.
- Along with impairing the right to freedom of speech and expression and the right to information, such internet suspensions hamper access to livelihood, education, and health.
- A First Information Report (FIR) has also been registered for the offence of sedition against a Manipur politician under Section 124-A of the Indian Penal Code, 1860 despite the Supreme Court's interim order dated May 11, 2022, in *S.G. Vombatkere v. Union of India*, which put the operation of Section 124-A in abeyance.
- News reports also suggest that Twitter accounts have been censored and withheld in India 'under a legal demand'. This has been executed in a manner such that there exists no public knowledge of the suspension and consequently no means to appeal against it.

Recommendations:

- Internet shutdowns must follow procedures and safeguards set down in law, including the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 and the Supreme Court's guidelines in *Anuradha Bhasin*.
- When an internet shutdown is imposed, a Review Committee must be constituted under Rule 2(5) of the Telecom Suspension Rules, which will review all internet suspension orders within 5 days of their issuance and record its findings on the legality of such orders.
- In *Anuradha Bhasin*, the Supreme Court held that internet suspensions are a 'drastic measure' which should only be exercised in 'necessary' and 'unavoidable circumstances', after evaluating the availability of less disruptive alternatives.
- The Supreme Court also held that the orders suspending internet services must be published.

4.4. Privacy concerns around state-surveillance

4.4.1. Use of CCTV cameras

The use of CCTV cameras in surveillance has been on the rise, with the supposed aim of preventing and reducing both crime and more minor offences, like traffic violations. Experts have repeatedly stated that CCTV cameras do not lead to an increase in security.[41]

[41]Jerry H. Ratcliffe & Jessica M. Rosenthal, "Video Surveillance of Public Places, 2nd Edition", Problem-Oriented Guides for Police Response Guide Series No. 4, Center for Problem-Oriented Policing at Arizona State University, June 2021, https://popcenter.asu.edu/sites/default/files/video_surveillance_of_public_places_2d_ed._9.1.22.pdf.

Concerns:

- CCTVs do potentially provide an avenue for the introduction of FRTs as an additional tool to monitor crime. This only multiplies the risk of false charges due to the inaccuracies inherent in these cameras and FRT.
- These cameras have also begun to be installed by governments in contexts other than safety, with some states using these cameras as an active surveillance network.

Common Cause, an advocacy group, along with Lokniti, Centre for the Study Developing Societies, and Lal Family Foundation, released the 2023 Status of Policing in India Report, which surveys public opinions on digital surveillance in India. The Report highlights the important impact CCTV surveillance has on the socio-political landscape of the country, with religious minorities and lower income groups being over-policed as a result of biassed surveillance.[42] It also discusses the use of CCTV surveillance and FRT to suppress dissent. Expert opinion on the submission of retrieved CCTV footage as evidence has stated that such surveillance can be misused for political purposes.

4.4.2. Undemocratic attempts at voter surveillance

In December 2023, the National Informatics Centre ("NIC") issued a tender titled 'Request for proposal for Empanelment of Agencies to Provide Surveillance & Monitoring Services, like for Elections, Examination etc.' for the acquisition and deployment of surveillance equipment, including drones and facial recognition technologies, to monitor election processes during the 2024 union and state elections.[43] The tender laid out plans for live-webcasting the voting and counting processes during elections, and setting up a "centralised command and control centre" to monitor activities in real time, in order to "*prevent unfair practices and maintain law and order at polling stations during elections.*" Subsequently on January 19, 2024, the Election Commission of India took notice of the tender and directed NIC to cancel it, noting privacy issues associated with voter surveillance.[44]

Concerns:

- While the ECI should be commended for upholding democratic principles and the right to privacy through its directions to withdraw the tender, implicated authorities must investigate how a tender with such far reaching implications on voter privacy was released in the first place.
- The tender notes ECI's interest in using surveillance tools and web-casting to monitor electoral processes, which is in direct contradiction to the Spokesperson's statement, and needs to be probed further.

[42] Anushka Jain, "The status of CCTV policing in India: 2023", Internet Freedom Foundation, May 01, 2023, https://internetfreedom.in/the-status-of-cctv-policing-in-india-2023.
[43] Sarasvati NT, "National Informatics Centre Outlines Plans To Surveil Polling Booths And Counting Halls During Elections." Medianama, January 9, 2024, https://www.medianama.com/2024/01/223-national-informatics-centre-election-surveillance-plan/.
[44] Disha Verma, "NIC withdraws voter surveillance tender: A small win for voter rights", Internet Freedom Foundation, January 22, 2024, https://internetfreedom.in/voter-surveillance-nic-withdraws-tender/.

- This is not the first time voter surveillance of this kind has been attempted. In May 2023, the ECI planned to pilot FRT-based voter verification in the Karnataka state elections.[45] Though it never materialised, any and all attempts at deploying voter surveillance tools in state or union elections need to be quashed at the outset.

4.4.3. DigiYatra's claims on data privacy and convenience raises doubts

With an aim to make air travel paperless and hassle-free, the DigiYatra Scheme was launched by the Ministry of Civil Aviation on June 8, 2017 by the then Minister of State for Civil Aviation, Shri Jayant Sinha. The scheme was put into operation in 3 Airports (namely New Delhi, Bengaluru, and Varanasi) in December 2022 and another 4 airports (namely, Vijayawada, Kolkata, Hyderabad, and Pune) in April 2023.

Concerns:

- Recently, concerns around DigiYatra have greatly exacerbated due to the unlawful and undignified manner in which it is being deployed at airports. Airline passengers across India are being ambushed and coerced into signing on to the "voluntary" Digi Yatra service and scan their faces at multiple airport check-points through deception and false information by private airport personnel and CISF staff.[46]
- Although the Policy states that airports using the DigiYatra Biometric Boarding System (BBS) will adhere to data protection laws and principles, the absence of a functional data protection regime raises serious doubts about this claim.
- Alarmingly, there are broad and ambiguous exceptions for sharing passenger data with government agencies, which contradict the principles of lawful processing, purpose limitation, data minimisation, accuracy, and storage limitation, among others.
- Furthermore, the policy fails to meet the requirements of necessity and proportionality in justifiably restricting the privacy of its users.[47]
- Finally, it is debatable whether the scheme will truly bring about an era of "easy boarding" considering the known inaccuracies of facial recognition technology, particularly when it comes to people of colour (including Indians) and women.[48]

[45] "Karnataka Assembly elections: ECI to pilot facial recognition tech in upcoming polls", Livemint, May 08, 2023, https://www.livemint.com/news/india/karnataka-assembly-elections-eci-to-pilot-facial-recognition-tech-in-upcoming-polls-11683526705081.html.
[46] Jagriti Chandra, "Centre's Digi Yatra enrolment takes off as airport security staff sign up flyers without their consent", The Hindu, January 5, 2024, https://www.thehindu.com/news/national/passengers-say-cisf-and-airport-staff-are-collecting-biometric-data-without-consent/article67710134.ece.
[47] Anushka Jain, "Part 1: The dangers of DigiYatra & facial recognition enabled paperless air travel #SaveOurPrivacy", IFF, January 18, 2022, https://internetfreedom.in/dangers-of-digiyatra.
[48] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots" , ACLU of Northern California, July 26, 2018, https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28?ref=static.internetfreedom.in
See also: "The Gender Shades Project", Algorithmic Justice League Project, http://gendershades.org/overview.html.

4.5. Misplaced digital interventions in the social security sector

On January 01, 2024, the Union Rural Development Ministry made the use of Aadhaar-Based Payment System ("ABPS") mandatory for the payment of wages to rural workers under the Mahatma Gandhi National Rural Employment Guarantee Act, 2005 ("NREGA"), and announced that non-compliance will be met with penalties.[49] Union and state governments have also been planning or piloting electronic surveillance of scheme workers through drones and facial recognition technologies.[50] Further, the NREGA Mobile Monitoring System ("NMMS") App which was made mandatory for workers to mark their attendance on last year, continues to be inaccessible and inaccurate, costing them their daily wage. Introducing technological interventions in the domain of social security and welfare delivery without addressing the digital divide and low rates of internet literacy in the country is a policy move that is bound to exclude and violate the fundamental rights of many.

Concerns:

- According to a statement by NREGA Sangharsh Morcha, as the Ministry of Rural Development began steps to make ABPS mandatory between 2022-23, NREGA account deletions shot up.[51] Workers whose bank accounts are not linked with their Aadhaar cards are being deleted from the central NREGA system, and forced to drop out of the scheme. Reportedly, while job cards of 4.74% of the total workers were deleted in 2021-22, job cards of nearly 19% of the total workers got deleted in 2022-23 and 7.72% of the workers in 2023-24. In less than two years, 7.6 crore job cards have been deleted from the system.[52] This is a large fraction of rural India which has fallen through the cracks due to the ABPS system, and is entitled to legal redress.
- In Bihar, Chhattisgarh, Jharkhand, Karnataka, Rajasthan, Uttar Pradesh, West Bengal and other states, the mandatory imposition of the NMMS App has caused many problems for NREGA workers, who have been demonstrating against it.[53] Due to glitches in the app or lapse of internet connectivity, workers are subjected to pay cuts and do not receive their compensation, which they are statutorily entitled to receive within 15 days.[54] While offline uploading of NMMS attendance and photographs has been introduced, the facility is still not operational in many areas.
- Further, surveillance of scheme workers raises several alarms for their rights to privacy, dignity, and free movement. According to a 2023 standard operating procedure

[49]"Will penalise states not MGNREGA workers if not linked with Aadhaar-based payment system: Minister", CNBC TV18, January 02, 2024, https://www.cnbctv18.com/economy/mgnrega-scheme-workers-giriraj-singh-states-aadhar-18701161.htm.
[50]Sobana K. Nair, "Now, drones to monitor MGNREGA worksites", The Hindu, August 18, 2023, https://www.thehindu.com/news/national/drones-to-monitor-mgnrega-worksites/article67205578.ece.
[51]"Aadhaar-Based Wages: 'Labelling 8.9Cr MGNREGA Workers 'Ineligible' Shows Utter Disregard for Poor'", NewsClick, January 04, 2024, https://www.newsclick.in/aadhaar-based-wages-labelling-89cr-mgnrega-workers-ineligible-shows-utter-disregard-poor.
[52]Sravasti Dasgupta, "MGNREGA: After Pushback on Aadhaar-Based Pay, Govt Defensive, Says May Consider Exemptions Case-by-Case", The Wire, January 02, 2024, https://thewire.in/labour/union-government-may-consider-case-by-case-exemptions-to-abps-mgnregs.
[53]Srinivas Kodali, "Why NREGA Workers Are Protesting Against an App", The Wire, February 20, 2024, https://thewire.in/tech/nrega-workers-nmms-app-protest.
[54]"Open Letter to MoRD, NREGA Sangharsh Morcha (English)", Srcibd, February 13, 2023, https://www.scribd.com/document/625693767/Open-Letter-to-MoRD-NREGA-Sangharsh-Morcha-English.

recently issued by the Ministry, drones may be deployed at NREGA sites for four types of monitoring: surveying the ongoing works, inspecting the completed works, impact assessment, and special inspection in case of complaints. Moreover, there are plans to launch facial recognition technology-based worker authentication at sites in 2024.[55] Privacy-invasive surveillance tools cannot be deployed in the absence of specific legal safeguards, which India currently lacks. Facial recognition-based authentication is also a highly inaccurate tool, and is more likely to inaccurately identify on the basis of gender, age and complexion, yielding low accuracy rates for a diverse Indian cultural landscape.[56] The Delhi Police has reported a match rate of around 80% on FRT systems, which is far from desirable.[57] The use of flawed authentication systems such as facial recognition may be potentially fatal to the scheme and lead to more and more workers falling through the cracks.

4.6. The social impact of emerging technologies

State and union governments are deploying artificial intelligence ("AI") on a large scale across sectors, spanning uses in urban administration, policing, surveillance, and welfare service delivery, to name a few.

Concerns:

- Such large-scale deployment of AI by government functionaries manifestly lacks transparency. State and union governments often do not make public the accuracy assessment processes or reports of the technologies they deploy across sectors. They do not reveal adequate information about the usage in the press releases or tenders. For instance, AI is being used in traffic management, city planning, waste management, and other urban administration issues under several flagship "Smart City" programmes, but little information is available about the kind of technologies used, the technology provider, the accuracy and cyber security measures taken, cost implications, or the data collected through AI.
- Research recommends that artificial intelligence, in its present form, should not be used in welfare service delivery by the union government, as the datasets are often not free from bias.[58] Use of AI in welfare schemes and by the police in the UK revealed three deficiencies.[59] An algorithm used by the Department for Work and Pensions led to dozens of people having their benefits removed; a facial recognition tool used by

[55]Risha Chitlangia, "Modi govt plans face authentication for MGNREGS attendance, eyes 2024 launch", ThePrint, December 17, 2024, https://theprint.in/india/governance/modi-govt-plans-face-authentication-for-mgnregs-attendance-eyes-2024-launch/1887436/.
[56]Aishwarya Jagani, "No facing away: Why India's facial recognition system is bad news for minorities", Unbias The News! September 28, 2021, https://unbiasthenews.org/no-facing-away-why-indias-facial-recognition-system-is-bad-news-for-minorities/.
[57] Anushka Jain, "From investigation to conviction: How does the Police use FRT?" Panoptic.in, July 02, 2021, https://panoptic.in/case-study/from-investigation-to-conviction-how-does-the-police-use-frt.
[58]Nidhi Singh, "Can AI ever be truly free from bias?", The Hindu Businessline, December 01, 2022, https://www.thehindubusinessline.com/opinion/can-ai-ever-be-truly-free-from-bias/article66210937.ece.
[59]"UK officials use AI to decide on issues from benefits to marriage licences", The Guardian, October 23, 2023, https://www.theguardian.com/technology/2023/oct/23/uk-officials-use-ai-to-decide-on-issues-from-benefits-to-marriage-licences.

the Metropolitan police made more mistakes recognising dark-skinned faces than light ones; an algorithm used by the Home Office to flag up sham marriages disproportionately selects people of certain nationalities.

- The manner of rapid and opaque deployment of AI in public sectors suggests that state and union governments may be using emerging technologies as “snake oil”, where an increasing number of interventions are being labelled “AI-powered” without the nodal authority necessarily understanding what that implies. Additionally, some use cases suggested by state governments such as using AI to detect distress on people’s faces or fatigue in drivers’ eyes, are not based in science, as AI globally does not yet possess the ability to be used in this manner.

Recommendations:

- At the outset, state and union governments must eradicate or, at the least, severely restrict the use of emerging technologies in the public sector, especially in the absence of research and understanding on the possible use cases of AI technology.
- Given the high instances of exclusion, bias and denial of service caused due to automated decision-making, emerging technology such as AI must be studied deeply, assessed for human rights impact and erroneous outcomes, and only deployed in a manner that is transparent, proportional, justifiable and accountable.

5. Abbreviations

- **Telecom Bill -** Draft Indian Telecommunication Bill, 2022
- **DoT** - Department of Telecommunications
- **TRAI** - Telecom Regulatory Authority of India
- **DPDPA, 2023** - Digital Personal Data Protection Act, 2023
- **IT Standing Committee** - Standing Committee on Communications and Information Technology
- **DIA** - Digital India Act
- **IT** - Information Technology
- **IT Rules, 2021** - The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
- **IT Amendment Rules, 2023** - Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023
- **SRDH** - State Resident Data Hub
- **UIDAI** - The Unique Identification Authority of India
- **APAAR** - Automated Permanent Academic Account Registry ID
- **ED** - Enforcement Directorate
- **AI** - Artificial Intelligence
- **BNS** - Bharatiya Nyaya Sanhita, 2023
- **BSS** - Bharatiya Sakshya Sanhita, 2023
- **BNSS** - Bharatiya Nagarik Suraksha Sanhita, 2023
- **MeitY** - Ministry of Electronics and Information Technology
- **MIB** - Ministry of Information and Broadcasting
- **GP** - Gram Panchayat
- **NBM** - National Broadband Mission
- **MoC** - Ministry of Communications
- **PM-WANI** - Prime Minister Wi-Fi Access Network Interface
- **PMGDISHA** - Pradhan Mantri Gramin Digital Saksharta Abhiyan
- **E2EE** - End-to-End Encrypted
- **P2P** - Peer-to-Peer
- **J&K** - Jammu & Kashmir
- **OTT** - Over-The-Top
- **FIR** - First Information Report
- **FRT** - Facial Recognition Technology

Internet Freedom Foundation
I-1718, Third Floor, Chittaranjan Park,
New Delhi 110019

Internet Freedom Foundation is a registered charitable trust that advocates for the digital rights of Indians. Our mission is to ensure the growth of digitisation with democratic rights guaranteed under the Constitution of India.

This brief is a result of the combined efforts of Associate Policy Counsels Tejasi Panjiar and Disha Verma, with assistance from Digital Literacy Intern, Anjney Mittal and Policy Intern, Vinamra Harkar.

Write to us at policy@internetfreedom.in.