International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838
Received: 20-01-2026, Accepted: 19-02-2026, Published: 06-03-2026
Volume 8, Issue 1, 2026, Page No. 154-159

From consent to compliance: How digital systems are reshaping the idea of constitutional freedom

Punit Yadav[1], Vishesh Paliwal[2], Veer Pratap Singh[1], Saloni Rajawat[1]
[1] National Law Institute University, Bhopal, Madhya Pradesh, India
[2] Damodaram Sanjivayya National Law University, Visakhapatnam, Andhra Pradesh, India

Abstract
The digital transition of India has dramatically changed how citizens interact with the State. What was earlier done through physical presence, discretion, and choice is increasingly routed through mandatory digital systems-such as OTP verification, biometric authentication, and service delivery on apps, and online only access to welfare, justice, and governance. This paper makes the argument that such a shift heralds a deeper constitutional transition from a framework premised on consent and voluntary participation to one of technological compliance and systemic compulsion.
Rather than dealing the issue through the perspective of any single Fundamental Right, this paper undertakes a structural analysis of constitution regarding how digital compulsion reinvents the basic meanings of freedom, autonomy, dignity, and democratic control. It shows how citizens are left with little choice but to give in to digital infrastructures in order to secure their basic services such as identity recognition, health services, and legal remedies. In that system, consent risks becoming procedural, not meaningful.
The paper further explores how this transformation weakens traditional ideas of accountability, filters constitutional relationships through these not clear technological architectures, and silently rearranges the balance of power between the citizen, the State, and private digital intermediaries. It contends that once access to rights becomes contingent on technological compliance, this threatens to shrink constitutional freedom to a coded permission structure, rather than a democratically guaranteed entitlement.
This paper, therefore, tries to initiate a larger constitutional discussion on whether the digital governance model of India is enhancing liberty or silently reorganizing it into a system of inevitable compliance by examining this emerging condition of "digital obedience."

Keywords: Digital constitutionalism**,** technological compliance**,** digital governance**,** constitutional freedom**,** digital obedience

Introduction

India's Digital India initiative, launched in 2015, promised empowerment through technology a seamless bridge between citizens and the State, where services like welfare subsidies, identity verification, and judicial access would flow effortlessly via apps, biometrics, and OTPs. A decade later, this vision has morphed into something far more insistent: a sprawling digital infrastructure that conditions every interaction on technological submission. What began as optional e-governance has hardened into mandatory gateways, Aadhaar-linked Direct Benefit Transfers (DBT), Digilocker for documents, UMANG for services, leaving citizens with no real choice but to comply or forfeit entitlements. This paper argues that such a shift marks a profound constitutional rupture: from a framework of consent and voluntary participation to one of systemic compulsion, where freedom is recast as coded permission rather than inherent entitlement.

Consider the everyday realities. A migrant labourer in rural Haryana, denied rations because her Aadhaar biometrics fail to authenticate amid dusty fingerprints or server glitches. A small trader in Delhi, unable to file GST returns without mandatory facial recognition that glitches on poor internet. Or a litigant approaching the e-Courts portal, compelled to upload personal data through third-party apps monitored under IT Rules, 2021. These are not mere technical hiccups; they embody "digital obedience," where access to constitutional goods, under Articles 14, 19, and 21, hinges on surrendering autonomy to opaque algorithms and private intermediaries. The Supreme Court's Puttaswamy judgement enshrined privacy as intrinsic to dignity and liberty, yet subsequent rulings like Puttaswamy II (2018) permitted Aadhaar's biometric mandates only under strict proportionality, necessity, minimal intrusion, safeguards. Today, that balance frays as digital compulsion proliferates unchecked.

This transformation demands structural scrutiny, not siloed Fundamental Rights analysis. Traditional constitutionalism posits the citizen-State relation as dialogic: consent legitimises authority, discretion enables choice, and accountability flows through human intermediaries. Digital systems invert this. Consent becomes procedural, a checkbox buried in app fine print, revocable in theory but illusory when opting out means starvation or exclusion. Compliance is engineered: OTPs that expire mid-transaction, apps that demand location data for "security," welfare schemes like PM-KISAN gated behind facial scans. As the DPDP Act, 2023, rolls out, even "legitimate uses" under Section 7(i); employment data processing without explicit consent, further entrenches this, blurring State mandates with corporate data hunger.

The paper's core contention is that mandatory digital infrastructures silently reorganise constitutional meanings. Autonomy shrinks to "datafied obedience"; dignity yields to surveillance architectures; democratic control filters through unaccountable platforms like Google or WhatsApp, now fiduciaries under DPDP. Puttaswamy warned of mass surveillance turning citizens into "transparent subjects," yet India's digital stack, Aadhaar, CoWIN, Aarogya Setu, normalises exactly this, with 2025 rulings on digital access

affirming Article 21 inclusion while exposing exclusionary risks for the digitally illiterate. Private actors, as "constitutional gatekeepers," mediate rights delivery, tilting power from Us the People to coded systems.

Structurally, the paper proceeds in three movements. Part I maps constitutional baselines, contrasting liberal consent with algorithmic compulsion. Part II dissects DPDP's consent-legitimate use dichotomy, revealing procedural traps in employment and welfare. Part III critiques hybrid architectures, State-private entanglements eroding accountability, before proposing "technological autonomy": opt-out rights, proportionality audits, judicial "digital disobedience" doctrines. Drawing on digital constitutionalism's global critique, it asks: Does India's model enhance liberty or encode obedience?

This is no Luddite lament; technology can liberate. But when constitutional freedom, preamble's justice, liberty, equality, becomes contingent on biometric submission, the Basic Structure trembles. As Justice Shri D.Y. Chandrachud noted in Puttaswamy, privacy is the "constitutional core of human dignity." Digital compulsion hollows it out, demanding urgent reclamation before India's Constitution becomes an analogue relic in a compliant republic.

Constitutional Freedom in a Data-filled State

The Indian Constitution, adopted in 1950, envisions freedom as an active, relational entitlement, citizens engage the State through choice, presence, and contestation, not pre-programmed submission. Articles 14, 19, and 21 form this edifice: equality before law, manifold freedoms of expression and movement, and life with dignity. Justice K.S. Puttaswamy (Retd.) v Union of India, the privacy judgment, crystallised this triad, declaring privacy not merely informational but existential: "the constitutional core of human dignity." Privacy, per the nine-judge bench, safeguards autonomy (self-determination), decisional privacy (intimate choices), and informational privacy (data control). Dissenting voices like Justice Chelameswar warned that unchecked surveillance renders citizens "transparent subjects," a prophecy unfolding in India's digital turn.

Puttaswamy I reframed Article 21's "personal liberty" through three prongs: legality (clear law), necessity (pressing aim), proportionality (minimal intrusion, balancing test). This imported global standards, European human rights law, US Fourth Amendment, into Indian doctrine, mandating judicial scrutiny of State intrusions. Yet the 2018 Aadhaar sequel (Puttaswamy II) tested these limits, upholding biometric mandates for welfare (Section 7 of Aadhaar Act) as "minimal" while striking private uses and mandatory linking for bank accounts, mobile numbers. Justice Chandrachud's concurrence cautioned: "The Aadhaar architecture creates... a regime of surveillance," permitting only "targeted" authentication, not mass data aggregation. Today's reality defies this: Aadhaar powers DBT (₹34 lakh crore disbursed by 2025), CoWIN vaccinations, even judicial e-filing, with authentication failures excluding millions.

This Datafied State alters constitutional grammar. Pre-digital, entitlements flowed through physical offices, discretion allowed waivers, appeals humanised denials. Now, freedom is infrastructural: coded into UIDAI servers, DigiLocker APIs, UMANG protocols. Consent, once meaningful (informed, revocable, granular), proceduralises under DPDP Act's Section 6, checkboxes amid 5000-word policies, where withdrawal risks service denial. DPDP's Section 7 defines Autonomy frays as "legitimate uses" deem employment data processable sans consent, echoing SPDI Rules' fadeout. Platforms like ONDC or BHIM, State-backed, mediate commerce and payments, positioning private entities as rights-gatekeepers.

Structurally, this inverts republican sovereignty. The Preamble's "We the People" cedes to "We the Algorithms," where Article 19(1) (a) expression filters through IT Rules' traceability (2021), and Article 21 dignity hinges on biometric success rates (UIDAI admits 2-5% failures). Digital constitutionalism, global discourse from PW Only IAS analysis, urges counter-architectures: rights-by-design, not compliance-by-default. In India, 2025 rulings like Amar Jain v UOI affirm digital access as Article 21-embedded, yet expose divides, rural illiteracy, and device poverty, affecting 40% population. Dignity demands not just inclusion, but refusal: a right to offline entitlements, analogue alternatives.

Puttaswamy's legacy hangs in balance. If privacy anchors liberty, digital compulsion, OTP for pensions, facial scans for rations, risks eviscerating it, turning constitutionalism into techno-administrative fiat. The paper next traces consent's mutation from liberal ideal to compliance ritual.

From Meaningful Consent to Systemic Compliance

Consent lies at the heart of liberal constitutionalism, a deliberate, informed act affirming the citizen-State compact. John Stuart Mill's harm principle, echoed in Article 21 jurisprudence, posits autonomy as inviolable unless overridden by compelling necessity. Puttaswamy I elevated this to constitutional stature: informational self-determination demands "free, informed choice," not coerced submission. Yet India's digital pivot transmutes consent from substantive right to procedural checkbox, rendering it hollow amid systemic compulsion.

The Digital Personal Data Protection Act, 2023 (DPDP), epitomises this shift. Section 6 mandates "free, specific, informed, unconditional, and unambiguous" consent on paper, robust. In practice, it buckles under infrastructure. Welfare apps like UMANG or PFMS demand Aadhaar-OTP linkage for pensions; revocation triggers exclusion from PM-KISAN or Ayushman Bharat. Section 7's "legitimate uses" exacerbate this: clause (i) permits employment data processing sans consent, for "safeguarding the employer from loss or liability." SNG Partners rightly flags the paradox: an employee's biometric scan for payroll becomes irrevocable once embedded in HR systems, blurring voluntary agreement with de facto mandate.

Contrast pre-digital regimes. Under the Information Technology Act's SPDI Rules, sensitive data like biometrics required written consent; non-compliance invited penalties. DPDP dilutes this, deemed consent for "employment purposes" swallow's background checks, performance metrics, and even post-termination retention. MZD Legal notes practical traps: applicant's data lingers in recruiter databases, processed by third-party processors without granular opt-outs. Consent withdrawable under Section 6(8)? Theoretically yes; practically, no, erasure risks unemployment verification denials, as former employers cite "liability safeguards."

This procedural framing echoes Foucault's disciplinary power: compliance engineered through frictionless interfaces masking coercion. A Delhi labourer authenticates

rations via Iris scan; failure (due to malnutrition-swollen eyes) means hunger. Consent? The app's "I Agree" button, unread amid 10,000-word terms. PW Only IAS frames this as "digital constitutionalism's failure", normative rights subordinated to techno-efficiency. Globally, GDPR's Article 7 empowers withdrawal without detriment; India's DPDP lacks equivalent teeth, with Section 13 grievance mechanisms routed through the very fiduciaries violating rights.

Structurally, this inverts accountability. Citizens, once sovereign choosers, become data subjects petitioning opaque Data Protection Officers under Section 10. Puttaswamy's proportionality crumbles: is OTP-mandated DBT "minimal intrusion" when alternatives exist? Courts have hinted no, vcn 2025 digital access rulings strike exclusionary mandates under Article 14, but enforcement lags. Consent, once constitutional bedrock, mutates into compliance ritual, priming the next analysis: DPDP's granular compulsions.

Digital Constitutionalism: Global Frames, Indian Context

Digital constitutionalism emerges as a critical response to platform power, seeking to embed human rights into code, algorithms, and data flows. Globally, scholars like Hofmann and Mihr frame it as "rights-by-design," countering Big Tech's "move fast, break things" ethos with proportionality and accountability. The Oxford Internet Institute's analysis traces its evolution: from GDPR's consent mandates to EU DSA's intermediary duties, challenging private architectures that rival State sovereignty. Yet this universalism frays in the Global South, where developmental imperatives collide with rights discourse.

In India, digital constitutionalism confronts a unique hybrid: State-led digital stacks (Aadhaar, UPI) entwined with private gatekeepers such as Google Pay and PhonePe. PWOnlyIAS captures the tension. Puttaswamy's privacy shield clashes with Digital India's efficiency mantra, birthing "constitutionalism with Indian characteristics." Unlike Europe's horizontal rights against platforms, India's flows vertically: citizen-State via mandatory e-KYC, where platforms execute State policy under IT Rules, 2021. The OUP article warns of "platform constitutionalism", WhatsApp's end-to-end encryption battles traceability mandates, yet India's context flips this: State compels private compliance, inverting liberal fears.

Societal constitutionalism, per Digi-Con's lens, offers traction: rights emerge not just from State/courts but communicative spheres, citizen pushback via #DeleteAadhaar or CoWIN data leak suits. Yet structural barriers persist: 2025 NITI Aayog reports 450 million offline Indians, rendering digital rights illusory. Puttaswamy II gestured here, limiting Aadhaar to "subsidy exclusion prevention," but 2025 welfare linkages like PM Garib Kalyan expand it surreptitiously. Global frames illuminate: China's Social Credit as dystopian foil; Estonia's e-residency as aspirational. India's midway, developmental surveillance, demands bespoke critique.

This adaptation reveals faultlines. Digital constitutionalism presumes agency; India's masses confront compulsion. Section 7 DPDP "legitimate uses" mirror EU "public interest," but without India's scale 1.4 billion data subjects, risks entrenching inequality. The paper turns next to DPDP's anatomy, exposing how statutory language codifies obedience.

The DPDP Act, 2023: Consent, Legitimate Uses, and Hidden Compulsions

The Digital Personal Data Protection Act, 2023, arrives as India's GDPR moment, yet laced with developmental caveats that tilt consent towards compliance. Enacted amid Puttaswamy's shadow, DPDP operationalises privacy through a fiduciary-principal dyad: Data Fiduciaries (State, employers, platforms) process Digital Personal Data with Data Principals' (citizens') nod or "legitimate use" exemptions. Section 4 permits processing for "lawful purpose," ostensibly safeguarding autonomy; Sections 5-6 demand notice and granular consent to be free, informed, and unconditional. SNG Partners dissect this finely: employment data under Section 7(i) bypasses consent for "purposes of employment" or "safeguarding from loss/liability," encompassing payroll biometrics, performance tracking, even post-termination retention.

Granularly, compulsions lurk. Section 7's exhaustive list of eight clauses; deems consent unnecessary for State functions (clause (a)), welfare (e), employment (i). Employer’s process health records sans explicit nod, citing "corporate espionage prevention"; platforms hoard transaction data under "service provision." MZDLegal flags the overlap with defunct SPDI Rules: sensitive data like biometrics, once requiring written consent, now slips into "legitimate uses," revocable only if not "disproportionately difficult." Section 6(8) withdrawal sounds empowering—yet Section 8 mandates fiduciaries ensure "accuracy for decisions affecting principals," binding employers to retain disputed data.

Hidden compulsions surface in architecture. Section 10 imposes Data Protection Officer Appointments for large fiduciaries; Section 8(6) demands security safeguards, breach notifications. Grievances under Section 13 route through the violator's mechanism, Data Principal petitions HR for payroll data misuse, facing reprisal. No independent ombudsman; appeals climb to Data Protection Board, appointed by executive. Puttaswamy's proportionality? Section 7 lacks necessity tests; "employment purposes" swallows’ surveillance, facial recognition for attendance, geofencing for field staff. Record flaw rightly terms this "constitutional mandate diluted": Article 21 dignity yields to statutory fiat, where opting out severs livelihood.

Judicial hints probe deeper. High Courts strike overreach, Karnataka HC (2024) voids mandatory corporate Aadhaar for non-subsidies, but DPDP's Section 17(2)(b) exempts State "security" processing, echoing Aadhaar's Section 33(2) surveillance. Employment exemplifies: SNG queries retention post-resignation, "liability safeguards" justify indefinite archiving, clashing Section 12 erasure rights. Consent, granular on paper, fractures under scale: 1.4 billion principals, millions of micro-fiduciaries. The Act codifies obedience, priming everyday compulsions next explored.

Employment, Welfare, and Everyday Infrastructures of Digital Obedience

Digital obedience manifests not in abstract statute but lived compulsion, employment records, ration cards, pension claims, all funnelled through unforgiving interfaces. SNG Partners lays bare the employment frontier: under DPDP Section 7(i), HR systems process biometrics for "attendance verification" sans consent, citing "liability safeguards." A factory worker in Noida scans irises daily; failure, due to fatigue or dust triggers docked pay. Withdrawal? Section

6(8) permits it, but erasure disrupts payroll audits, risking termination. Post-resignation, data lingers indefinitely: background checks for new jobs cite "corporate espionage prevention," trapping mobility. This isn't choice; it's infrastructure lock-in, where livelihood hinges on data surrender.

Welfare schemes amplify the coercion. PM Garib Kalyan Anna Yojana demands Aadhaar-POS authentication; 2025 UIDAI data logs 12% failure rates in rural authentication, excluding 50 million from grains. A widowed farmer in Bihar forfeits rations not for ineligibility, but biometric mismatch, swollen fingers from labour. Alternatives? Offline vouchers exist on paper, scrapped post-DBT "efficiency." Ayushman Bharat gates hospitalisation behind facial recognition; glitches deny chemo to cancer patients. Puttaswamy II permitted Aadhaar for "subsidy exclusion prevention," but 2025 expansions: PM-KISAN OTPs, Ujjwala LPG via DigiLocker, stretch "minimal intrusion" to breaking.

Everyday touchpoints entrench obedience. GST portals mandate facial scans for returns; e-Courts require Aadhaar e-signatures, filtering Article 39A justice through servers. UMANG super-app aggregates 1200+ services, each demanding location data "for security." MZD Legal flags processor chains: State contracts private vendors (IDFC, Airtel) for authentication, diffusing accountability, citizen grievances ping corporate helplines, not tehsildars. The digitally illiterate, elderly, tribals face compounded exclusion: NITI Aayog's 2025 survey pegs 35% rural adults' offline, rendering Article 21's "life with dignity" conditional.

These infrastructures invert dignity. Pre-digital, a Sub-Divisional Magistrate exercised discretion; now, algorithms rule, UIDAI's e-KYC rejects "liveness" fails without appeal. Foucault's panopticon finds digital form: perpetual visibility for entitlements, anonymity for the powerful. Section 13 grievances circle back to fiduciaries welfare beneficiary petitions MeitY-approved apps for data misuse. Judicial nudges emerge: Madras HC (2024) mandates offline PDS alternatives, but compliance lags. Employment and welfare, as constitutional gateways, expose obedience's banality-freedom rationed by code, not right.

Private Platforms as Constitutional Gatekeepers

Private platforms- Google, WhatsApp, PhonePe, have metastasised into constitutional intermediaries, mediating rights delivery under State compulsion. DPDP casts them as Data Fiduciaries or Processors (Sections 2(k), 8), processing transaction data, location traces, even voice notes sans granular consent via Section 7's "service provision" clause. MZD Legal dissects this: UPI apps demand Aadhaar linkage for merchant payments; non-compliance halts small businesses under ONDC mandates. A vegetable vendor in Haryana scans QR codes daily, her turnover data feeding NPCI servers, revocable? Only if she forfeits digital economy access.

IT Rules, 2021, amplify gatekeeping: intermediaries must trace originators (Rule 4(2)), breaking end-to-end encryption for "national security. WhatsApp's 2021 challenge invoked Article 19(1)(a): traceability chills expression but Delhi HC deferred to legislative policy. Platforms now police content: grievance officers (Rule 3A) field takedown requests, filtering Article 19 freedoms through corporate triage. DPDP Section 13 routes data grievances to these same officers, creating fox-guarding-henhouse dynamics. A user querying bank details via chatbot petitions Meta for erasure, facing algorithmic deflection.

This hybridity fractures accountability. Platforms execute State mandates, Aadhaar authentication via Airtel Payments Bank, CoWIN data via AWS yet liability diffuses. Puttaswamy II struck private Aadhaar uses, but 2025 welfare portals (PM-SVANidhi) route loans through Razorpay, harvesting applicant biometrics under "legitimate uses." rule of law flags the Article 21 breach: decisional privacy evaporates when loan approval hinges on Google Location History "verification." Platforms profit-transaction fees, ad targeting, while citizens surrender autonomy.

Structurally, this upends republicanism. Article 12's "State" expands de facto; private code rivals' public law. Digital constitutionalism's global fix-EU DMA's interoperability, falters here: India's scale demands developmental shortcuts, birthing obedience. A gig worker on Swiggy consents to geofencing or starves; refusal means delisting. Judicial glimmers pierce: Kerala HC (2024) voids mandatory platform rating disclosures, citing dignity. Yet platforms endure as gatekeepers, priming privacy's next defence.

Privacy, Autonomy, and the Right to Say no

Privacy under Article 21 is no mere shield against intrusion; it is the constitutional heartbeat of autonomy, the power to refuse, to remain opaque, to author one's data destiny. Puttaswamy I etched this indelibly: privacy comprises informational self-determination (data control), decisional privacy (intimate choices), and spatial privacy (bodily integrity). Justice Chandrachud invoked Kantian dignity: "The integrity of the body and the sanctity of the mind can exist on the foundation that each individual... has the inalienable right to preserve his or her mind and body inviolate." Digital obedience shreds this. Aadhaar's iris scans for rations invade spatial privacy; UPI apps' perpetual transaction logs erode informational autonomy. Refusal? Starvation or bankruptcy.

Autonomy fractures under compulsion. DPDP Section 7's "legitimate uses" deem employment biometrics processable sans nod, HR tracks keystrokes for "productivity," geofences field staff for "attendance." SNG Partners exposes the trap: post-resignation erasure (Section 12) clashes with "liability safeguards," leaving ex-employee's data-prisoners. A software engineer in Bengaluru contests facial recognition payroll data; withdrawal servers, PF claims, and throttling mobility. The rule of law rightly decries this as "constitutional mandate betrayed", Article 21's liberty demands a right to say no, not opt-in or exclude binaries.

The "right to say no" demands doctrinal birth. Puttaswamy II gestured, striking mandatory private Aadhaar, but 2025 realities mock it: Digi Yatra facial scans at airports, mandatory for "seamless travel." Courts nudge forward: Bombay HC (2024) voids corporate wellness app mandates, affirming decisional privacy over "health compliance." Yet statutory voids persist. Global cues illuminate GDPR's Article 21 objection rights, California's CCPA erasure mandates. India needs analogues: DPDP amendments for "objection to legitimate uses," offline entitlements under Article 14 proportionality.

Structurally, digital compulsion infantilises citizens, algorithms presume incompetence, demanding submission for "protection." Article 19(1)(a) expression chills under

traceability; dignity yields to liveness checks failing veiled women. A right to refusal restores agency: proportionality audits for mandates, State-funded offline kiosks, judicial "digital disobedience" precedents. Without it, privacy hollows into permission slips, priming accountability's reclamation next.

Reimagining Accountability in Hybrid Public-Private Architectures

Accountability, the bedrock of constitutional democracy, traditionally flows vertically: citizens hold the State answerable through writs, RTI, and elections. Digital governance disrupts this flow by dispersing power horizontally across a hybrid mesh of State agencies and private intermediaries. When a ration card is denied due to an Aadhaar authentication failure, is the liable entity UIDAI (State), the Point of Sale vendor (private), or the telecom provider (network failure)? This diffusion creates an accountability vacuum where citizens are bounced between bureaucratic silence and corporate customer care bots.

The DPDP Act, 2023, exacerbates this by routing grievances (Section 13) back to the very Data Fiduciaries, causing harm. An employee contesting biometric misuse must petition HR; a welfare beneficiary denied a pension must lodge a ticket on the UMANG app. SNG Partners notes the conflict of interest: Fiduciaries investigate themselves, with appeals climbing to a Data Protection Board appointed by the central executive, lacking the independence of a constitutional court or an autonomous regulator like the original concept of the Data Protection Authority. This mirrors the "administrative state" critique, but stripped of procedural safeguards like natural justice.

Hybrid architectures further obscure liability. State platforms like CoWIN or ONDC run on private cloud infrastructure (AWS/Azure) and use third-party APIs (payment gateways, chatbots). MZD Legal highlights that under DPDP, Data Processors (the private vendors) are accountable only to Fiduciaries, not Principals. A data breach at a private processor handling health records for a government hospital leaves the citizen with no direct remedy against the negligent vendor. The State claims sovereign immunity or contractual indemnity; the vendor claims "processor" status. The citizen is left destitute.

Reimagining accountability demands piercing this veil. We need a doctrine of "joint and several constitutional liability" for State-mandated digital systems. If a private intermediary executes a public function like disbursing welfare or authenticating identity, it must be amenable to writ jurisdiction under Article 226, amenable to RTI, and subject to algorithmic audits. The "State" under Article 12 must expand to encompass these "digital instrumentalities." Furthermore, the grievance redressal mechanism must be independent of fiduciaries, an Ombudsman model with suo motu powers, accessible offline.

Without these structural shifts, digital governance remains a "black box" where power is exercised without consequences. Accountability must be reclaimed from code and contracts, restored to constitutional forums where "We the People" can demand answers, not just submit tickets.

Towards a Constitutional Grammar of Technological Autonomy

The transition from digital obedience to constitutional freedom requires more than piecemeal litigation; it demands a new constitutional gram mar, concepts and doctrines tailored to the datafied state. "Technological autonomy" must emerge as a distinct facet of Article 21, defined not just as privacy (the right to be left alone) but as the affirmative power to negotiate one's engagement with digital systems. This implies a "right to analogue alternatives", a constitutional mandate that essential services (welfare, justice, health) must remain accessible through non-digital channels, ensuring that technology remains a tool of facilitation, not a gatekeeper of existence.

This grammar rests on three pillars. First, a revitalized doctrine of unconstitutional conditions. The State cannot condition the receipt of a constitutional benefit (ration, pension, legal remedy) on the waiver of a fundamental right (privacy, informational self-determination). Current coercion "scan iris or starve" violates this. Courts must apply strict scrutiny: is the digital mandate the *least restrictive measure*? If an offline verification works (as it did for decades), the digital compulsion is disproportionate.

Second, algorithmic due process. Administrative law principles, audi alteram partem (right to be heard), reasoned orders, must translate to code. When an algorithm denies a claim (e.g., a "fraud" flag in a DBT transfer), the system must provide an explainable reason and a human appeal layer. "Computer says no" cannot be a constitutionally valid administrative order. This requires statutory mandates for algorithmic audits and "human-in-the-loop" safeguards for high-stakes decisions affecting liberty or livelihood.

Third, fiduciary constitutionalism. The concept of the State as a fiduciary holding data in trust for citizens must move from academic theory to enforceable law. This imposes a duty of loyalty: The State cannot use data collected for welfare (e.g., PDS) for surveillance (e.g., criminal profiling) or commercialisation (e.g., selling datasets). DPDP's Section 7 "legitimate uses" must be read down by courts to exclude purposes that violate this fiduciary bond.

Finally, we need to embed "digital disobedience" as a form of democratic dissent. The right to delete an app, to use encryption, to refuse biometric linking without suspicion, these are modern expressions of civil liberty. Just as the freedom of speech includes the right to remain silent, the freedom of digital existence must include the right to disconnect. Reclaiming this grammar is essential to prevent the Constitution from becoming a legacy document, irrelevant to the coded realities of modern power.

Conclusion: Reclaiming Freedom Beyond Coded Permission

The trajectory of India’s digital governance, from the promise of empowerment to the reality of "digital obedience" signals a quiet but profound constitutional crisis. As this paper has argued, the shift is not merely administrative but structural. We are witnessing the displacement of the republican ideal of the active, consenting citizen by the "compliant subject," whose access to the most basic elements of life and liberty is contingent upon successful authentication by opaque, often private, technological systems. The constitutional guarantee of dignity is being re-written as a coded permission structure; rights are no longer inherent, but algorithmic outputs.

The Digital Personal Data Protection Act, 2023, rather than checking this transformation, largely codifies it. By expanding "legitimate uses" and proceduralising consent into a hollow ritual, the law creates a framework where

compliance is the default and autonomy the aberration. This "datafied state" blurs the lines between welfare and surveillance, public duty and private profit, leaving the citizen vulnerable in a hybrid architecture of power that evades traditional accountability.

Yet, the Constitution is resilient. The path forward lies in reclaiming its text to confront these digital realities. We must insist that technology be an enabler of rights, not a gatekeeper. This requires a robust judicial re-interpretation of Article 21 to include "technological autonomy" the right to refuse, the right to offline alternatives, and the right to meaningful, un-coerced consent. It demands legislative courage to subject the State's digital appetites to strict proportionality and fiduciary bounds.

Ultimately, the question is whether India will remain a republic of citizens or become a database of subjects. If we are to preserve the freedoms envisioned in 1950, we must reject the inevitability of digital obedience. We must assert that in the hierarchy of Indian democracy, the Constitution still sits above the code.

References

1. De Gregorio G, Radu R. Digital constitutionalism in the new era of Internet governance. International Journal of Law and Information Technology,2022:30:68-87.
2. Mill JS. On Liberty. Oxford University Press, 1998, 80-81.
3. Celeste E. Digital Constitutionalism: A New Systematic Theorisation. International Review of Law, Computers & Technology,2019:33(1):76-93.
4. De Gregorio G. From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society. European Journal of Legal Studies,2019:11(2):65-86.
5. Gill N, *et al*. The Digital Poor: Tech-Exclusion in India's Welfare State. Economic and Political Weekly,2025:59:45-52.
6. Reddy C. Digital Constitutionalism in the New Era of Internet Governance. International Journal of Law and Information Technology,2022:30(1):68-87.
7. Teubner G. Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory? Constitutionalism and Democracy,2004:100:3-28.
8. Balkin JM. The Cyberspace Constitution: The New Rules of Digital Speech and Privacy. Harvard University Press, 2023, 3-25, 59-104.
9. Cohen JE. Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019, 7-36, 181-225.
10. Zuboff S. The Age of Surveillance Capitalism. PublicAffairs, 2019, 8-24, 376-401.
11. Pasquale F. The Black Box Society. Harvard University Press, 2015, 3-18, 140-172.
12. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, 2010, 127-157.
13. Richards NM. Intellectual Privacy. Oxford University Press, 2015, 21-45, 95-123.
14. Floridi L. The Ethics of Information. Oxford University Press, 2013, 67-89.
15. Brownsword R. Law, Technology and Society: Re-imagining the Regulatory Environment. Routledge, 2019, 15-48, 121-160.
16. Yeung K. Algorithmic Regulation: A Critical Interrogation. Cambridge University Press, 2021, 55-92.
17. Teubner G. Constitutional Fragments: Societal Constitutionalism and Globalization. Oxford University Press, 2012, 39-67, 135-162.
18. Habermas J. Between Facts and Norms. MIT Press, 1996, 82-131.
19. Susskind R. Online Courts and the Future of Justice. Oxford University Press, 2019, 63-101.
20. Mayer-Schönberger V, Cukier K. Big Data. Houghton Mifflin Harcourt, 2013, 97-123.