

4. Digital Constitution- Polity

DoT walks back Sanchar Saathi pre-installation directive following uproar

Following widespread backlash over privacy and surveillance concerns, the government revoked its order mandating the pre-installation of the 'Sanchar Saathi' app on mobile phones. This incident has reignited the debate on "Digital Constitutionalism," which advocates extending constitutional safeguards like liberty, accountability, and the rule of law to regulate both State surveillance and the power of private digital platforms.

The Sanchar Saathi Revocation

The Incident- The Indian government recently revoked an order that required mobile phone manufacturers to mandatory pre-install the Sanchar Saathi app on all devices starting from 2026.

Reason for Revocation- The decision came within 48 hours of the initial order due to intense backlash from-

Civil Society & Opposition- Concerns regarding unclear data collection, lack of consent, mass surveillance, and unlimited data storage.

Global Tech Giants- Companies like Apple resisted the move.

Current Status- The government clarified that the app is voluntary. Users retain the freedom to install, delete, or deactivate it.

About Sanchar Saathi- Purpose & Features

It is a citizen-centric telecom security platform developed by the Department of Telecommunications (DoT).

Core Purpose- To empower subscribers to secure digital identities, combat fraud, and prevent the misuse of telecom resources (stolen devices/fake SIMs).

Key Modules-

Chakshu (Fraud Reporting)- Allows citizens to proactively report suspected fraudulent communications (Scam calls/SMS, fake KYC messages, financial fraud).

CEIR (Device Security)- Integrates with the Central Equipment Identity Register. It allows users to block and trace lost/stolen phones across all networks using the unique IMEI number, rendering the stolen device unusable.

TAFCOP (Identity Verification)- Enables users to check all mobile connections issued under their name/identity proof. Users can report or disconnect unauthorized numbers.

The Controversy- Critics labeled the mandatory pre-installation a "snooping app". It was argued to violate the Right to Privacy by removing user choice and consent.

Digital Constitutionalism

Digital Constitutionalism refers to extending fundamental constitutional values—liberty, dignity, equality, accountability, and the rule of law—into the digital ecosystem.

Core Philosophy- In a world where technology mediates governance, these principles must guide the design, deployment, and regulation of digital systems.

Key Pillars

Protection of Digital Rights- Safeguarding privacy, freedom of expression, and access to information against misuse by State and private actors.

Accountability of Platforms- Holding digital companies responsible for transparent data usage and non-discriminatory algorithms.

Digital Sovereignty- A nation's control over its digital space, data residency, and infrastructure in a globalized environment.

Judicial Oversight- Courts must review digital laws/algorithms to ensuring compliance with constitutional principles.

Digital Inclusion- Ensuring equal access and digital literacy regardless of socio-economic background.

Digital Systems Mediating Governance

Modern administration relies on systems that authenticate identity but also create permanent digital trails.

Biometric Databases

Aadhaar– Unique Identification Authority of India.

Digi Yatra– Facial Recognition System for airports.

Concern– These create capability for large-scale surveillance.

Automated & Predictive Algorithms

Predictive Policing– Forecasting crime locations/perpetrators.

Automated Welfare– Targeting beneficiaries for schemes.

Credit Scoring– Financial institutions determining loan eligibility.

Concern– These often operate without transparency or human appeal mechanisms.

Comparison– Classical vs. Digital Constitutionalism

Feature	Classical Constitutionalism	Digital Constitutionalism
Primary Focus	Regulates visible state actions (laws, executive orders, police action).	Regulates invisible, algorithm-driven decision-making and data flows.
Key Mechanism	Judicial Review checks government power.	Focuses on Algorithmic Accountability, privacy by design, and data ethics.
Decision Makers	Human officials (legislators, executives).	Predictive Algorithms (forecasting behavior) and Biometric Identifiers.
Data Source	Official records and legal documents.	Continuous Metadata Collection (location logs, device IDs, behavioral traces).
Scope of Power	Limits the State/Government.	Limits both the State and Private Tech Platforms.

Evolution of Constitutional Values

Original Values (19th Century)

Response to absolute monarchy.

Focused on Written Constitution, Rule of Law, and Separation of Powers.

Goal– Limit the State and prevent arbitrary authority.

Contemporary Evolution– Shifted from "Negative" (restricting state) to "Positive" (state must promote welfare).

Centrality of Dignity– Focus on Liberty, Equality, and Human Dignity.

The "State-Link" Myth– Modern constitutionalism is no longer just about the State. Globalisation has extended norms to international institutions and private corporations. It creates a plural/fragmented ecosystem where rights operate across borders.

The Need for Digital Constitutionalism in India

Post-Puttaswamy Mandate– Privacy is a Fundamental Right (Article 21; *Justice K.S. Puttaswamy v. Union of India*, 2017). All digital systems must pass the tests of Necessity, Proportionality, and Fairness.

Balancing Development with Rights

The JAM Trinity (Jan Dhan–Aadhaar–Mobile)– Brought 520 million people into the formal economy. Reduced welfare leakages by ₹2.7 lakh crore. *Challenge*– These benefits must now operate within a

Privacy by Design framework to prevent the erosion of rights.

Global Regulatory Models

European Union (Rights-Based)

GDPR– Establishes "Right to Explanation" and "Right to be Forgotten".

AI Act– Risk-based model classifying AI (Unacceptable, High, Limited risk) with mandatory audits for high-risk systems.

United States (Decentralised/Market-Based)– Lacks federal privacy law. Relies on state laws like CCPA (California) which allow opt-outs but vary in protection.

Global South (Sovereignty-Based)– Focus on Digital Sovereignty. Must balance privacy with inclusion (e.g., relying on biometric welfare systems like DBT).

Critical Challenges & Concerns

Surveillance & The Chilling Effect– Silent monitoring via metadata and facial recognition creates a

climate of fear. *Example*– Facial recognition at 2023 Delhi protest sites deterred mobilization.

Rising Cybercrime vs. Proportionality

Cybercrime Stats– Cases rose from **15.9 lakh in 2023** to **20.4 lakh in 2024**. *Issue*– The government uses these stats to justify intrusive tools (like mandatory Sanchar Saathi), raising proportionality concerns.

Weak Privacy Protections– DPDP Act, 2023– Criticized for giving the State broad exemptions. Consent is reduced to a "forced click-through".

Algorithmic Bias (Black Box)–Outcomes are often opaque. *Example*– Digi Yatra (2024) showed higher false positives for women and minorities.

Tech Failure & Exclusion–Reliance on biometrics excludes elderly/disabled.

Example– **Jharkhand (2024)** saw ration denials due to biometric failure, forcing emergency manual verification.

Federal Stress–Centralized surveillance projects (like Sanchar Saathi mandate) often bypass State governments and Parliamentary debate.

Way Forward– Institutionalising Digital Constitutionalism

Comprehensive Surveillance Law– Enact legislation requiring judicial warrants and independent audits for all state surveillance.

Strengthen DPDP Act– Remove blanket exemptions for the government; enforce data minimization.

Algorithmic Accountability– Mandate Impact Assessments and bias audits for high-risk AI in policing and welfare.

Independent Digital Rights Commission– A statutory body to investigate violations and block unconstitutional tech deployment.

Judicial Expansion– Recognize "Right to Explanation" and "Right to Human Review" under Article 21.

Constitutional Compliance– Ensure all digital governance respects Articles 14 (Equality), 19 (Freedom), and 21 (Life/Liberty).

Technical Standards– Adopt BIS/ISO standards for reliability in AI and biometrics before public deployment.

Source– <https://www.thehindu.com/news/national/government-withdraws-mandatory-sanchar-saathi-pre-installation-on-phones-after-backlash/article70352971.ece>