The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

TELECOM SECURITY THROUGH SANCHAR SAATHI: IS VOLUNTARINESS ENOUGH?

~Utkarshika Srivastava

ABSTRACT

*Governments today increasingly govern not by issuing orders, but by building digital systems that shape how people communicate. Sanchar Saathi, a platform created by the Government of India to prevent telecom fraud and help users recover lost phones, is one such system. By allowing phones to be blocked across networks using their International Mobile Equipment Identity ("**IMEI**"), the platform directly affects access to communication, even though it is presented as a voluntary and user-driven service. This article asks a simple question: when the State controls access to communication through digital infrastructure, are consent and basic transparency enough?*

This article argues that they are not. While the Government has listed the permissions required by the app and emphasised that users choose whether to use it, these measures only explain how people enter the system. They do not explain what happens after. These key questions remain unanswered. How long is user data kept? Who can access it? How are mistakes reviewed? And what limits prevent temporary restrictions from continuing indefinitely?

Using Articles 19 and 21 of the Constitution of India, the article examines Sanchar Saathi through the Supreme Court's approach to communication rights, particularly the requirement that restrictions must be limited in time, proportionate, and open to review, as laid down in Anuradha Bhasin v Union of India. It also considers how exemptions under the Digital Personal Data Protection Act, 2023 reduce the role of consent and make stronger safeguards necessary.

The article concludes that in public digital systems, consent cannot replace law. Technology may enable governance, but only clear legal limits and accountability can make it constitutional.

Keywords: *Public Digital Infrastructure; Sanchar Saathi; IMEI Blocking; Digital Personal Data Protection Act, 2023; Consent; Telecom Regulation; Constitutional Rights; Digital Governance*

INTRODUCTION

Suppose you wake up to discover that your smartphone no longer connects to any network. No calls, no internet, no explanation. You have not violated any law, nor has any court heard your case. Yet, your access to communication has been effectively disabled by an administrative system operating in the background of India's telecom infrastructure. When digital systems underpin everything from employment to banking to public services, their disruption ceases to be a simple technical glitch and

instead operates as a regulatory act with real constitutional implications.

It is within this evolving landscape of digital governance that the Government of India introduced Sanchar Saathi. Conceived as a digital public infrastructure framework, Sanchar Saathi encompasses multiple telecom governance functions, including mechanisms for fraud prevention, device authentication, and network-level controls such as International Mobile Equipment Identity ("**IMEI**") blocking.[1] The initiative seeks to address legitimate concerns surrounding telecom fraud, identity misuse, and the growing vulnerability of users in an increasingly digitised ecosystem. On its face, the framework appears both necessary and responsive to contemporary challenges.

Yet, as digital governance expands, the legal questions it raises grow more complex. Sanchar Saathi operates not merely as a consumer-facing application or website, but as an infrastructural mechanism capable of disabling devices and regulating access to communication networks.[2] Such power, even when exercised for legitimate ends, implicates constitutional concerns that go beyond individual consent or user choice. The issue is not whether the State may collect data to provide public services. That necessity is well established. The deeper question is how transparently and how lawfully such power is structured, limited, and supervised.

In response to public concern, the Government has now publicly announced that Sanchar Saathi is voluntary and that users may choose whether to install the application or access services through its website.[3] It has also published a privacy policy that lists the permissions required for the app's functioning, including access to call logs, SMS data, storage, and camera functions.[4] This disclosure has been cited to counter claims of opacity. However, transparency in public digital infrastructure cannot be reduced to the disclosure of front-end permissions alone. What remains largely unexplained is what happens after this data is collected. How is it processed? Who may access it across departments? How long is it retained? What safeguards exist against repurposing or error? And what remedies are available to citizens if harm occurs?

These unanswered questions assume greater significance in light of India's evolving data protection framework. The Digital Personal Data Protection Act, 2023 explicitly exempts certain State actions undertaken for security and fraud prevention from ordinary consent and notice requirements.[5] Exemptions of this kind may be understandable in principle. However, they also weaken the idea that

---

[1] Department of Telecommunications, Government of India, *Sanchar Saathi Portal* https://sancharsaathi.gov.in\ accessed 10 January 2026.
[2] Department of Telecommunications, Government of India, '*Central Equipment Identity Register (CEIR)*' https://sancharsaathi.gov.in/Home/Ceir.jsp\ accessed 10 January 2026.
[3] Ministry of Communications, Government of India, *Government removes mandatory pre-installation of Sanchar Saathi App* (Press Information Bureau, 3 December 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198110&reg=3&lang=2 accessed 10 January 2026.
[4] Department of Telecommunications, Government of India, *Sanchar Saathi App Privacy Policy* https://sancharsaathi.gov.in/Home/app-privacy-policy.jsp#:%7E:text=For%20Android%3A%20Following%20permission%20are,device%20along%20with%20purpose%3A accessed 10 January 2026.
[5] Section 17(1)(c), Digital Personal Data Protection Act, 2023 (India)

consent can meaningfully limit State power. If the law does not clearly regulate how data is processed, retained, or shared behind the scenes, then consent becomes a formality rather than a protection.

This concern is particularly acute where Sanchar Saathi enables IMEI blocking, a measure that operates at the infrastructural level of communication. Blocking a device does not regulate speech content, yet it directly determines whether speech can occur at all. The Supreme Court's approach to restrictions on communication infrastructure has been guided by concerns of temporality and review. In *Anuradha Bhasin v Union of India*, the Court held that such measures must be limited in duration, proportionate in scope, and subject to periodic oversight.[6] Sanchar Saathi does not impose a system-wide shutdown. Yet its device-blocking architecture allows access to communication to be disabled without clear limits on duration or mandatory review. The lack of statutory time limits, independent audits, or appellate review mechanisms weakens the safeguards that this jurisprudence seeks to enforce.

What makes these concerns more acute is that the entire system rests within one administrative entity. The Department of Telecommunications designs the system, operates it, enforces its consequences, and oversees grievance handling.[7] Even within a voluntary scheme, such institutional consolidation increases the risk of error and arbitrary decision-making and offers little by way of effective redress. A wrongful device block can therefore restrict access to communication without any prior hearing or independent mechanism for review.

This article does not challenge the legitimacy of telecom fraud prevention or the State's authority to collect data for public purposes. Nor does it suggest that initiatives like Sanchar Saathi are constitutionally suspect merely because they process personal information. The concern lies elsewhere. It lies in the absence of clearly articulated legal limits governing how data is used, retained, reviewed, and repurposed once it enters the system. While the Digital Personal Data Protection framework recognises broad governmental exemptions for security and fraud prevention, those exemptions also underscore the need for independent safeguards where backend processing remains largely opaque. By examining Sanchar Saathi through the lenses of transparency, consent, infrastructural control, and proportionality, this article argues that effective digital governance requires more than technological capability. It requires legal restraint. In public digital infrastructure, consent cannot replace law. It must operate within it.

This article is structured in four parts. The first part explains how Sanchar Saathi is designed and how it operates as a system of public digital governance over telecom networks. The second part examines the issues of transparency and consent and questions whether existing disclosures adequately regulate how data is processed behind the scenes. The third part analyses the constitutional implications of the scheme and focuses on proportionality, procedural safeguards, and the review of measures that affect access to communication. The final part places this discussion within the Digital Personal Data

[6] *Anuradha Bhasin v Union of India* [2020] 3 SCC 637 (Supreme Court of India) [70–71], [79].
[7] Department of Telecommunications, Government of India, *Grievance Redressal – Sanchar Saathi* https://sancharsaathi.gov.in/Home/Grievance.jsp\ accessed 10 January 2026.

Protection framework and proposes recommendations to strengthen oversight, accountability, and restraint in public digital systems.

CHAPTERS

A. SANCHAR SAATHI AS PUBLIC DIGITAL INFRASTRUCTURE

a) FROM CONSUMER SERVICE TO INFRASTRUCTURAL CONTROL

Sanchar Saathi is often described as a public-facing digital service that helps users report lost mobile phones or identify fraudulent connections. While this description is accurate, it is incomplete. Framing Sanchar Saathi solely as an application or a grievance redress platform understates the nature of the power it exercises. In practice, the framework operates at the level of telecom infrastructure that enables the State to regulate access to mobile networks themselves.

At the core of Sanchar Saathi lies the Central Equipment Identity Register ("**CEIR"**), a system that allows mobile devices to be identified and blocked across telecom networks using their numbers.[8] Once an IMEI is blocked, the device is rendered incapable of connecting to cellular networks, regardless of the user, the service provider, or the location. This form of control does not merely assist the user. It alters the conditions under which communication is technically possible.

This distinction matters. A consumer-facing digital service connects users with the system by sharing information, allowing reporting, or enabling voluntary interaction. By contrast, infrastructural systems shape access itself. They operate in the background, often invisibly, but with consequences that are immediate and difficult to reverse. When a device is blocked through Sanchar Saathi, the effect is not advisory or informational. It is disabling. The user's ability to communicate is curtailed not through a judicial order or an adjudicatory process, but through an administrative system embedded within telecom networks.

Understanding Sanchar Saathi as public digital infrastructure rather than merely an application is therefore essential. It clarifies why the scheme raises constitutional and governance questions that go beyond data protection or consumer consent. The concern is not only about what data is collected, but about how technological systems are used to exercise regulatory power over communication itself.

b) VOLUNTARINESS AND ACCESS PATHWAYS

In response to public criticism, the Government of India has repeatedly emphasised that Sanchar Saathi is voluntary. Users are not required to install the application, and services such as reporting lost devices or checking mobile connections can be accessed through the official website. The earlier requirement to pre-install the application was taken back which reinforced the narrative that

[8] *Central Equipment Identity Register* (n 2).

participation in the scheme is a matter of choice.[9]

Voluntariness, however, does not fully capture the legal implications of the system. While a user may choose whether to engage with Sanchar Saathi, the consequences of that engagement are not similarly discretionary. Once a request is made, such as blocking a device, the resulting action operates at the network level and affects access to communication in a direct and immediate manner. The user's initial choice does not determine how long the block remains in place, what review mechanisms exist, or how errors are corrected.

Moreover, access through the website relies on forms of implied consent. Users are deemed to accept backend data processing practices by using the service, even though the legal and technical details of those practices are not fully articulated. This model resembles browsewrap consent mechanisms commonly found in private digital services, but its use in a public digital infrastructure context raises distinct concerns. When the State provides an essential remedial service, the choice is often between consenting to opaque backend processes or forgoing the service altogether.

Voluntariness also does not address the institutional structure of the scheme. The fact that a user opted into the system does not mitigate the impact of a wrongful block or the lack of procedural safeguards that follow.

For these reasons, voluntariness cannot be treated as a constitutional shield. It may explain how users enter the system, but it does not resolve questions about how power is exercised once they do. When digital governance operates at the level of infrastructure, the focus must shift from entry points to accountability structures. Choice alone cannot substitute for legal limits, review mechanisms, and institutional checks.

B. TRANSPARENCY AND CONSENT

a) WHAT THE GOVERNMENT DISCLOSES

Public criticism of Sanchar Saathi has often focused on the permissions sought by its mobile application. In response, the Government of India has pointed to the existence of a publicly available privacy policy that enumerates these permissions in detail.[10] The policy specifies that the Android version of the application seeks access to phone call status, call and Short Message Service ("**SMS**") logs, storage and files, camera access for scanning IMEI numbers, and the ability to send messages for verification purposes. These disclosures are presented as evidence that the framework is transparent and that users are adequately informed before engaging with the service.

It would be inaccurate to dismiss this disclosure as insignificant. Unlike many private digital services that bury permissions within dense terms of service, Sanchar Saathi does place its permission

[9] *Government removes mandatory pre-installation* (n 3).
[10] *Privacy Policy* (n 4).

requirements in the public domain. Media reports and security analysts have noted that several of these permissions are categorised as "dangerous" under Android's permission framework, given their potential to expose sensitive personal data.[11] The fact that these concerns have been openly discussed, and that the Government has responded by emphasising voluntariness and choice, indicates an awareness of public scrutiny rather than an attempt at concealment.

Transparency, however, is not a binary concept. It is not satisfied merely by listing what an application can access on a user's device. In public digital infrastructure, transparency must be assessed in relation to the nature of the power being exercised. Where a system operates at the level of telecom infrastructure and enables device-level controls, the disclosure of front-end permissions addresses only a narrow slice of the governance framework. It tells the user what data may be accessed at the point of interaction, but it says little about how that data is treated once it enters the system.

This distinction is crucial. Front-end disclosures are visible, legible, and familiar to users accustomed to navigating mobile applications. Back-end governance, by contrast, determines how authority is exercised in practice. It governs the movement of data across systems, the duration of its retention, the entities that may access it, and the safeguards that exist against misuse or error. It is at this level that the real scope of State power is defined.

b) WHAT REMAINS OPAQUE

While the Sanchar Saathi privacy policy enumerates permissions, it provides limited insight into what happens after data is collected. The policy does not clearly distinguish between data that is directly provided by the user and data that is generated by the system itself in the course of delivering services. For instance, metadata created through device blocking requests, verification processes, or fraud detection mechanisms may be far more revealing than the initial inputs supplied by the user. Yet the governance of such generated data remains largely unexplained.

Equally unclear are the standards governing data processing and retention. The policy does not specify how long different categories of data are retained, whether retention periods vary based on purpose, or when deletion is triggered. Without clear sunset clauses or publicly defined retention timelines specific to Sanchar Saathi, users have no real way of knowing how long their data continues to exist within the system. Data collected for an immediate remedial purpose may persist within systems long after that purpose has been fulfilled.

The question of access further complicates the picture. Sanchar Saathi operates within a broader telecom governance ecosystem involving the Department of Telecommunications, Telecom Service Providers, and potentially other State agencies engaged in fraud prevention and security functions.

[11] Reuters, *India's Sanchar Saathi App Requests Dangerous' Permissions, Say Analysts* (28 November 2025) https://www.reuters.com/technology/indias-sanchar-saathi-app-requests-dangerous-permissions-say-analysts-2025-11-28/ accessed 10 January 2026.

The privacy policy does not clearly articulate which entities may access backend data, under what legal authority, or subject to what procedural safeguards. Without this information, it is difficult for users to assess the extent to which their data may circulate beyond the immediate service they sought to use.

This opacity is not necessarily the result of bad faith. Large-scale digital governance systems are complex, and backend processes are often distributed across multiple technical and administrative layers. However, complexity does not absolve the State of the obligation to articulate limits. Where power is exercised invisibly and at scale, transparency must extend beyond surface-level disclosures to include the rules that govern backend operations.

The absence of publicly articulated standards also makes meaningful accountability difficult. If a device is wrongly blocked, or if data is misused, the lack of clarity around backend processes makes it challenging to identify responsibility or seek remedy. Transparency, in this sense, is not only about informing users. It is about enabling oversight, audit, and redress.

c) Consent as a Trigger, not a Safeguard

The Government has frequently relied on user consent to justify Sanchar Saathi's data practices. Users choose whether to install the application or access services through the website, and by doing so, they are deemed to have agreed to the terms set out in the privacy policy. In ordinary consumer-facing digital services, such consent often serves as the primary legal basis for data processing.

In the context of public digital infrastructure, however, consent plays a more limited role. It may justify the initial collection of data, but it does not meaningfully regulate how State power is exercised after that point. This limitation becomes clear when access to essential remedial services is involved. When the State offers mechanisms for recovering lost devices or preventing fraud, users are not choosing between equivalent alternatives. They must either accept backend data processing that is only partially explained or forgo the service altogether. In such circumstances, consent reflects necessity rather than genuine choice.

The use of the Sanchar Saathi website further illustrates this point. While the website does not employ a traditional browsewrap agreement in the private-law sense, it relies on implied consent mechanisms. Users are deemed to accept backend data processing by submitting requests through the platform, even though the full scope of such processing is not clearly articulated. This model may be adequate for low-stakes informational services, but it becomes problematic when the service enables infrastructural controls that affect access to communication.

The Digital Personal Data Protection Act, 2023 further weakens the reliance on consent. By exempting State processing for fraud prevention and security from notice and consent requirements, the Act limits the capacity of user consent to act as a real constraint on State power. In such a framework, consent triggers data processing but does not govern its scope or consequences.

This does not mean that consent is irrelevant. Rather, it means that consent cannot be the sole safeguard in systems that exercise infrastructural power. In public digital infrastructure, consent must operate alongside clearly articulated legal limits that govern retention, access, review, and remedy. Without such limits, consent risks becoming a procedural formality rather than a substantive protection.

Seen in this light, the transparency concerns surrounding Sanchar Saathi are not about the absence of disclosure, but about its incompleteness. Front-end permissions tell only part of the story. The more consequential questions lie in the backend, where data is processed, decisions are made, and access to communication is ultimately shaped. These questions cannot be answered by consent alone. They require clear legal limits and institutional accountability.

C. CONSTITUTIONAL CONCERNS: INFRASTRUCTURAL CONTROL AND PROPORTIONALITY

a) COMMUNICATION INFRASTRUCTURE AND CONSTITUTIONAL PROTECTION

Indian constitutional law has long recognised that the freedom of speech and expression under Article 19(1)(a) of the Constitution of India is not confined to the content of speech alone.[12] It extends to the means through which speech is made possible.[13] Access to communication networks, devices, and infrastructure increasingly determines whether individuals can meaningfully exercise their expressive freedoms in a digital society.

Smartphones today are not merely consumer goods. They function as gateways to speech, association, information, and economic participation. Blocking a device at the network level does not regulate what a person says, but it directly affects whether they can speak, communicate, or access digital services at all. The constitutional question is not whether the State regulates speech itself, but on how control over infrastructure shapes the ability to communicate and participate in everyday life.

Sanchar Saathi operates precisely at this infrastructural layer. Through the CEIR, it enables IMEI based blocking of devices across telecom networks. While preventing misuse and fraud is a legitimate objective, the mechanism used directly affects access to communication. For this reason, the scheme raises constitutional concerns, even though it is presented as a technical or administrative measure.

Importantly, the constitutional concern here is not that the State lacks the power to regulate telecom infrastructure. Such regulation is well within its authority. The concern is whether this power is exercised within clearly defined limits that respect proportionality, procedural fairness, and accountability. Where infrastructural control is exercised without clear temporal boundaries or review mechanisms, the risk of constitutional overreach increases.

---

[12] Constitution of India art 19(1)(a).
[13] *Bennett Coleman & Co v Union of India* [1973] 2 SCC 788 (Supreme Court of India) [28–29].

b) ANURADHA BHASIN AND THE REQUIREMENT OF TEMPORALITY AND REVIEW

The Supreme Court's in *Anuradha Bhasin v Union of India* held that restrictions affecting access to the internet must satisfy the requirements of legality, necessity, and proportionality, and must be subject to periodic review.[14] Crucially, the Court emphasised that even justified restrictions cannot be indefinite.[15]

While *Anuradha Bhasin* arose in the context of internet shutdowns, the principles articulated by the Court are not limited to blanket suspensions of services. The judgment recognised access to communication networks as integral to the exercise of fundamental rights under Articles 19 and 21. It also underscored that the longer a restriction operates without review, the greater the risk of constitutional infirmity.

Sanchar Saathi does not impose a general shutdown of services. However, its IMEI-based blocking can still have lasting effects. Once a device is blocked, access to telecom services is cut off, even if the original reason for IMEI blocking no longer applies. Because the framework does not prescribe clear review timelines or sunset clauses, a temporary measure can quietly become permanent.

This absence of time limits sits uneasily with the approach adopted in *Anuradha Bhasin*. Time limits and periodic review were treated as constitutional safeguards precisely because they prevent temporary measures from hardening into routine controls. When systems that regulate access to communication operate without such limits, it becomes impossible to tell whether a restriction continues to serve its purpose or has become excessive.

The issue is not that every instance of device blocking must be short-lived. Rather, it is that the law must clearly specify when and how such measures are reviewed, extended, or withdrawn. Without such clarity, infrastructural controls may continue even after their original purpose has ended.

c) ABSENCE OF PROCEDURAL SAFEGUARDS

Another constitutional concern arises from the absence of robust procedural safeguards within the Sanchar Saathi framework. The absence of independent review mechanisms raises concerns that extend beyond proportionality and into questions of institutional design. When authority is concentrated within a single framework, it heightens the risk of error and arbitrariness, even within a scheme that is technically voluntary. These procedural gaps are compounded by deeper questions about institutional design, which the next section addresses.

If a device is wrongly blocked due to incorrect data, mistaken identity, or technical error, the consequences are immediate and tangible. The affected individual's ability to communicate is

[14] *Anuradha Bhasin v Union of India* [2020] 3 SCC 637 [Supreme Court of India] [68–71], [79].
[15] Ibid.

impaired without prior notice, hearing, or independent review. While grievance mechanisms exist, they operate within the same institutional framework that imposed the restriction in the first place.

Indian constitutional law has consistently treated procedural safeguards as central to the legitimacy of State action. Measures that affect fundamental interests demand independent scrutiny. Without appellate review or external audits, infrastructural controls are left to operate on trust rather than accountability.

This concern is magnified by the scale at which digital systems operate. Errors in manual decision-making affect individuals one at a time. Errors in automated or semi-automated systems can affect large numbers of users simultaneously. Without independent oversight, such errors may persist undetected.

Voluntariness does not resolve this problem. Even when users opt into a system, they do not waive their constitutional right to fair procedure. The risk of wrongful deprivation of access to communication remains, regardless of whether participation was initially optional.

d) INSTITUTIONAL CONSOLIDATION AND THE NEED FOR ACCOUNTABILITY

Compounding these concerns is the consolidation of multiple functions within a single administrative framework. The Department of Telecommunications designs the architecture of Sanchar Saathi, oversees its operation, enforces network-level consequences, and addresses grievances arising from its use. There is no independent body tasked with reviewing decisions, auditing backend processes, or evaluating proportionality over time.

Such institutional consolidation is not unique to Sanchar Saathi, nor is it inherently unconstitutional. However, when combined with infrastructural control over communication networks, the absence of external checks becomes constitutionally significant. Accountability mechanisms are most necessary where power is exercised invisibly and at scale.

The lack of independent oversight also interacts with the broader data protection framework. As discussed earlier, exemptions under the Digital Personal Data Protection Act, 2023 reduce the role of consent and notice in constraining State data processing. In such a context, institutional safeguards assume even greater importance. Where statutory limits are weak, procedural checks must compensate.

From a constitutional perspective, the concern is not the existence of a fraud prevention mechanism, but the absence of clearly articulated limits on how far and for how long its effects may extend. Without independent review, sunset clauses, or mandatory audits, infrastructural controls risk becoming normalised rather than exceptional.

This section thus demonstrates that the challenge posed by Sanchar Saathi is not one of intent, but of design. Constitutional compliance in digital governance requires not only legitimate objectives, but

also restraint, review, and accountability built into the system itself.

D. THE DPDP FRAMEWORK AND THE LIMITS OF VOLUNTARINESS

a) GOVERNMENT EXEMPTIONS UNDER THE DPDP ACT

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive attempt to regulate personal data processing through a statutory framework. At a general level, the Act introduces important principles relating to purpose limitation, data minimisation, and accountability. By establishing institutions such as the Data Protection Board of India, the Act attempts to move data governance away from ad hoc executive control and toward a more structured framework.[16]

However, the framework adopts a markedly different approach when it comes to State processing of personal data. Section 17 of the DPDP Act, read with the Digital Personal Data Protection Rules, permits the government to process personal data for specified purposes such as national security, public order, and fraud prevention without adhering to the usual requirements of notice or consent.[17] Rule 23 further allows the government to require any data fiduciary to provide personal data for such purposes, without prior judicial authorisation or proportionality review.[18]

These exemptions are not unusual in comparative data protection law. States routinely reserve broader powers where public interests such as security or fraud prevention are involved. The legitimacy of Sanchar Saathi's objectives, particularly in addressing telecom fraud and misuse, is therefore not in serious dispute. The concern lies elsewhere. If consent and legal scrutiny are weakened, the system must rely more heavily on other safeguards to prevent misuse.

In this regulatory context, Sanchar Saathi operates within a framework where the State enjoys wide discretion over data use once processing is triggered. While the DPDP Act provides general safeguards, it does not impose scheme-specific obligations relating to retention limits, deletion timelines, or independent audits for systems such as Sanchar Saathi. As a result, the rules governing backend data processing are shaped largely by executive decisions rather than clear legislative mandates.

b) WHY EXEMPTIONS INCREASE THE NEED FOR SAFEGUARDS

Statutory exemptions do not reduce the need for constitutional scrutiny. They make strong institutional safeguards even more important, especially when consent and notice are set aside in the public interest.

In the case of Sanchar Saathi, exemptions under the DPDP Act weaken the assumption that user

[16] Digital Personal Data Protection Act, 2023 (India) s 18.
[17] ibid s 17.
[18] Digital Personal Data Protection Rules, 2025 (India) r 23.

consent can meaningfully constrain backend data processing. Once a user initiates a request, the subsequent handling of data operates largely beyond the user's control and, in some respects, beyond ordinary statutory visibility. Without independent audits, periodic disclosures, or mandatory review mechanisms, users and oversight bodies alike are left with limited insight into how the system evolves over time.

Comparative data protection regimes illustrate a different balance. In the European Union, for instance, law enforcement and security-related data processing is often accompanied by strict record-keeping obligations, independent supervisory authorities, and periodic review requirements. These mechanisms acknowledge that while exemptions may be necessary, they must be counterbalanced by heightened accountability.

The problem, therefore, is not that the State processes data for fraud prevention. It is that the legal framework does not clearly specify how that processing is constrained once consent and notice are set aside.

c) VOLUNTARINESS IS NOT A CONSTITUTIONAL SHIELD

Participation in a public scheme does not amount to a waiver of fundamental rights, nor does it absolve the State of its obligation to act within clearly defined legal limits. Even where individuals voluntarily engage with State-run digital systems, the Constitution continues to demand proportionality, procedural fairness, and accountability. These requirements are structural. They attach to the exercise of public power, not to the presence or absence of user choice.

In this sense, voluntariness explains how the system is triggered but it cannot serve as a constitutional defence for how the system operates. The State's obligation to provide clear limits, independent oversight, and effective remedies persists even when participation is optional.

This section has shown that the core challenge posed by Sanchar Saathi is not voluntariness or consent in isolation. It is the absence of clearly articulated legal boundaries governing backend data use in a system that affects access to communication infrastructure. Addressing this gap requires moving beyond consent-based models and toward a governance framework grounded in statutory limits, independent oversight, and meaningful review.

CONCLUSION

Sanchar Saathi reflects an important shift in the Indian State's approach to digital governance. Rather than merely regulating conduct at the surface level, it operates directly on the infrastructure that enables communication itself. Its objectives are legitimate. Telecom fraud and device misuse pose real harms, and the State is entitled, indeed obligated, to respond with effective technological solutions. The constitutional concern examined in this article does not lie in the existence of such a system, nor in the collection of data that is genuinely necessary to make it function.

The real difficulty lies in how power is structured and controlled once they are in place. Sanchar Saathi reflects a wider problem in public digital infrastructure, where transparency at the user interface and formal consent are treated as sufficient, while the rules governing backend operations remain unclear and weakly regulated. As this article has shown, listing permissions or emphasising voluntariness does little to answer the more consequential questions. How long is data retained? Who may access it? How are errors reviewed? What limits prevent temporary measures from becoming permanent controls?

The constitutional analysis demonstrates that these questions are not peripheral. Measures that affect access to communication infrastructure engage Articles 19 and 21 of the Constitution of India, even when they are framed as technical or administrative tools. The Supreme Court's insistence in *Anuradha Bhasin v Union of India* on temporality, proportionality, and periodic review reflects a deeper constitutional principle: infrastructural control must be disciplined by clear limits and ongoing accountability. Sanchar Saathi, as currently designed, departs from this discipline by operating without statutory sunset clauses, independent review mechanisms, or clearly articulated backend governance standards.

The Digital Personal Data Protection Act, 2023 provides a necessary backdrop to this discussion. While the Act introduces an important framework for data protection, its exemptions for State processing reduce the practical role of consent and notice in constraining public power. In such a regulatory environment, the absence of scheme-specific safeguards becomes more, not less, significant. Voluntariness may explain how users enter the system, but it cannot serve as a constitutional shield for how the system operates thereafter.

Taken together, these concerns lead to a simple conclusion. Public digital infrastructure cannot be judged lawful just because it works or because users click "agree." It must operate within clear legal limits and under meaningful oversight. Without these constraints, even well-intentioned systems can allow exceptional State power to quietly become the norm.

RECOMMENDATIONS

The constitutional concerns identified in this article do not suggest that Sanchar Saathi should be dismantled. Instead, it highlights the need to rethink how the scheme is governed. The following recommendations aim to preserve the scheme's objectives while bringing it within clearer constitutional bounds.

First, **statutory sunset clauses and review timelines should be introduced for IMEI-based blocking**. Any restriction on access to communication infrastructure should operate for a defined period and be subject to mandatory review. Once the original basis for blocking has lapsed, the continuation of such restrictions should be permitted only upon fresh authorisation.

Second, **clear data retention and deletion standards specific to Sanchar Saathi should be publicly articulated**. These standards should distinguish between data provided by users and data

generated by the system, specify retention periods for each category, and mandate deletion once the relevant purpose has been fulfilled.

Third, **independent oversight mechanisms must be institutionalised.** This could take the form of periodic audits conducted by an external authority, with summaries placed in the public domain. Oversight should extend to backend data processing, not merely front-end compliance.

Fourth, **a meaningful appellate or review mechanism should be established for cases of wrongful blocking or prolonged restriction.** Grievance redress should not remain entirely within the same administrative framework that designs and enforces the system. Independent review is essential to mitigate error and arbitrariness at scale.

Finally, **exemptions under the Digital Personal Data Protection Act should not operate in isolation.** Relaxing consent and notice in the public interest should trigger stronger duties of accountability, documentation, and review, not their absence.

Sanchar Saathi demonstrates the State's growing capacity to govern through digital infrastructure. Whether this capacity strengthens constitutional democracy or reshapes it depends on the legal limits that accompany it. Effective digital governance is not achieved by asking how much technology can do, but by deciding, in law, how far it should be allowed to go.