DIGITAL SEARCH POWER UNDER THE INCOME TAX ACT, 2025: FROM PHYSICAL SEIZURE TO VIRTUAL INTRUSION

Khushbu Choudhary, Advocate, Rajasthan High Court, Jodhpur

ABSTRACT

The proposed Income Tax Act, 2025, seeks to significantly expand the investigative powers of tax authorities by introducing the concept of "virtual digital space," granting them extensive access to an individual's digital life. This comment examines the constitutionality of these proposed powers, tracing the evolution of search and seizure jurisprudence in India from a state centric interpretation to a robust, individual-centric fundamental right to privacy. It critically analyses the Act's provisions against the backdrop of landmark Supreme Court decisions, particularly *Justice K.S. Puttaswamy* v. *Union of India*. The central thesis argues that while modernizing tax enforcement is necessary, the Act, in its current form, lacks essential procedural safeguards, such as a judicial warrant requirement and the principle of data minimalization. This transforms a legitimate investigative tool into a mechanism for unconstitutional surveillance, posing a great threat to informational privacy, the right against self-incrimination under Article 20(3), and the very fabric of a free and democratic society. The comment concludes by recommending a framework of robust constitutional and statutory safeguards to balance the state's fiscal interests with the citizen's fundamental rights.

I. INTRODUCTION

The relentless march of technology has shifted the focus of human interaction, commerce and record-keeping from physical to digital realm. In response the state's investigative apparatus which has come up with the Income Tax Act, 2025 (hereinafter referred as "the Act") represents a watershed moment in this evolution. The Act introduces the expansive concept of "virtual digital space," empowering the income tax authorities to search and seize data not just from physical devices but from cloud server, social media accounts, encrypted communications and any other form of digital existence. The legislative measures aim to equip the state to effectively combat tax evasion in an increasingly digital economy.

This expansion of power is not a mere technical update; it is a profound constitutional challenge. It forces a confrontation between the state's legitimate interest in revenue collection and the citizen's fundamental right to privacy and protection against self-incrimination. The central issue this comment address is whether the new expansion of digital search powers represents a necessary and proportionate modernization of tax investigation or an unconstitutional foray into pervasive state surveillance, fundamentally altering the relationship between the citizen and the state. This enquiry is critical, for the manner in which we regulate the state's access to our digital lives will define the contours of liberty in the 21st century.

II. DOCTRINAL EVOLUTION OF SEARCH AND SEIZURE IN INDIA

The constitutional validity of the provisions of this Act can only be assessed by tracing the jurisprudence of search, seizure, and privacy law in India. This journey reveals a transformative shift from a narrow, property centric view to a broad, dignity centric understanding of individual autonomy.

A. *M.P. Sharma vs. Satish Chandra*: The State- Centric Genesis

The earliest constitutional examination of search and seizure occurred in *M.P. Sharma vs. Satish Chandra*[1], where and eight judge bench of the Supreme Court adopted a starkly state-centric approach. The court held that the search and seizure power was not violative of the right against self-incrimination under Article 20(3) of the Constitution, reasoning that such compulsion was not "testimonial" in nature. The court also refused to import a fundamental

[1] AIR 1954 SC 300

right to privacy into the Indian Constitution viewing it an alien concept.

B. *Kharak Singh* and *Gobind*: The Nascent Recognition of Privacy

The first doctrinal shift appeared in *Kharak Singh vs. State of Uttar Pradesh*[2], where the Supreme Court, while upholding police surveillance regulations, acknowledged in a minority opinion that the right to "personal liberty" under Article 21 included aspects of privacy. This idea was further developed in the case of *Gobind vs. State of Madhya Pradesh*[3], where the court explicitly recognised a qualified right to privacy, holding that it could be infringed upon only if there was a compelling state interest and the intrusion was narrowly tailored.

C. *District Registrar and Collector vs. Canara Bank*: Protecting financial Privacy

The jurisprudence took a significant leap in *District Registrar and Collector vs. Canara Bank*[4], a case of immense relevance to tax investigation. The Supreme Court held that the State's power to demand inspection of bank's records constituted a serious invasion of customer's privacy. It ruled that the privacy extends to financial records and that any state intrusion into this sphere must be justified by compelling public interest and be backed by adequate procedural safeguards.

D. *Justice Puttaswamy vs. Union of India*: The constitutional Apotheosis of Privacy

The constitutional landscape was irrevocably altered by the nine-judge bench in *Justice K.S. Puttaswamy vs. Union of India*[5]. The court unanimously held that the privacy is a fundamental right, intrinsic to personal life and liberty under Article 21 and as a part of freedoms guaranteed by Part III of the constitution. This case fundamentally rebalanced the scales, creating a high constitutional threshold for any state action that infringes upon informational self-determination.

E. The Pegasus Era: Confronting Digital Surveillance

The evolution of Constitutional thought has now entered the era of digital surveillance, exemplified by concerns surrounding technologies like Pegasus spyware. The judiciary is

[2] AIR 1963 SC 1295
[3] (1975) 2 SCC 148
[4] (2005) 1 SCC 496
[5] (2017) 10 SCC 1

increasingly confronted with the unique challenges posed by invisible, pervasive and continuous digital monitoring. This context underscores that the threat to liberty is no longer confined to physical search of a home but extends to the silent expropriation of one's entire digital person. Indian constitutional law is thus moving inexorably towards recognizing a right to informational autonomy in the digital age, a right that Income Tax Act, 2025, directly implicates.

III. THE INCOME TAX ACT, 2025 AND THE SCOPE OF "VIRTUAL DIGITAL SPACE"

The new Act amending the Income Tax Act, 1961, by introducing a definition of "virtual digital space" that includes, but is not limited to, data held on cloud servers, social media profiles, email accounts, encrypted messaging applications, and any other form of electronically stored information, regardless of its physical location. This grants authorities the power to demand access, including passwords and encryption keys, to this entire digital ecosystem.

This statutory innovation is constitutionally problematic on several grounds. Firstly, the definition is excessively vague and overbroad potentially encompassing every facet of an individual's digital life, from personal correspondence to professional data. Such vagueness grants unbridled discretion to executive authorities, violating the principle that laws restricting fundamental rights must be precise and narrowly tailored.[6] Secondly, and most alarmingly the Act Fails to mandate a judicial warrant as a precondition for such an intrusive search. It allows a high-ranking tax official to authorize a digital search based on a "reason to believe," a standard far lower than the probable cause required for a judicial warrant. This absence of prior judicial scrutiny removes a critical safeguard against arbitrary state action, effectively making the executive the sole arbiter of the necessity and scope of the intrusion.

IV. ARTICLE 20(3) AND COMPELLED PASSWORD DISCLOSURE

The Act's provision for compelling the disclosure of passwords and encryption keys raises a direct conflict with the right against self-incrimination enshrined in Article 20(3). The established doctrine distinguishes between testimonial compulsion, which is prohibited, and the production of physical evidence, which is permitted.[7] The state can compel an accused to

[6] Shreya Singhal vs. Union of India, (2015) 5 SCC
[7] State of Bombay vs. Kathi Kalu Oghad, AIR 1961 SC 1808

provide fingerprints or a blood sample, as this is considered providing “physical” evidence.

However, a password is not analogous to a fingerprint. A password is a product of the mind, a piece of knowledge, a memory, a key created and held within the mental faculty of the individual. Compelling its disclosure is not the mere production of a physical object; it is forcing an individual to reveal the contents of their mind to unlock a trove of personal information. This act of revealing a secret is inherently testimonial. It is a communication of knowledge that can lead to incriminating evidence.

V. CONSTITUTIONAL CONCERNS RAISED BY DIGITAL SEARCH POWERS

The powers envisaged in the Act trigger a cascade of constitutional concerns that extends beyond procedural irregularities. The Act threatens to render the *Puttaswamy* judgment a hollow promise. The right to privacy is not merely the right to be left alone; it creates a chilling effect on free speech and association, as citizens may self-censor their communications and activities for fear of state scrutiny. The sanctity of digital home, the digital diary, and the digital conversation is as crucial to a dignified existence as their physical counterparts.

The Act is symptomatic of a broader trend towards “surveillance constitutionalism,” where the state increasingly seeks pervasive algorithmic and digital access to its citizens’ lives. Such a regime creates a digital panopticon, where the state’s gaze is constant, invisible and potentially limitless. This fundamentally alters the citizen-state relationship from one of trust and liberty to one of suspicion and control, which is antithetical to a democratic polity.

A core tenet of proportionality test is that the state must use the least intrusive means to achieve its objective. The Act fails this test spectacularly. It contains no principle of data minimization, which would require authorities to access and retain only the data strictly relevant to investigation. Instead, it permits a digital dragnet, scooping up vast amount of irrelevant, intimate, and privileged information, from medical records to personal photographs, in the hunt of financial data.

VI. CRITICAL COMMENT

While modernization of tax enforcement is a legitimate and necessary state objective in the digital economy, unrestricted access to virtual digital spaces without robust procedural safeguards risks converting fiscal investigation into constitutionally impermissible digital surveillance. The state's interest in preventing tax evasion, however compelling, cannot be a justification for the wholesome evisceration of fundamental rights. The architecture of the Act, in its present hypothetical form, is constitutionally unsustainable as it fails the proportionality test laid down in *Puttaswamy.*

To remedy these constitutional infirmities, a new framework is essential. Any law permitting digital searches must incorporate the following non-negotiable safeguards:

- Judicial Warrant Requirement: No digital search should be conducted without a warrant issued by a judicial magistrate, based on written application demonstrating probable cause that a specific tax offense has been committed.

- Specificity and Narrow Tailoring: the warrant must specifically describe the data to be searched, the account to be accessed, and the time period under review. Fishing expeditions must be statutorily prohibited.

- Data minimalization principle: The law must mandate that authorities only access, seize and retain data that is strictly necessary and relevant to the specific investigation. All non-relevant data must be immediately and permanently deleted.

- Protection of Privilege: A clear mechanism must be established to protect privileged communication from being accessed or used.

VII. CONCLUSION

The journey of Indian Constitutional Law from *M.P. Sharma* to *Puttaswamy* has been a journey towards embracing individual dignity and autonomy as core constitutional values. The new Income Tax Act, 2025, threatens to reverse this progress, pushing India towards a surveillance state under the guise of fiscal efficiency. The Legislature must recognise that technology can be a tool for empowerment or a tool for oppression. By introducing a law that balances investigative needs with inviolable constitutional rights, India can set a global standard for democratic governance in the digital age. Failure to do so will not only endanger the right to privacy but will corrode the very foundation of a society governed by the rule of law.