LEGAL IMPLICATIONS OF DIGITAL PUBLIC INFRASTRUCTURE IN INDIA (AADHAAR; UPI; DIGI LOCKER): BALANCING INNOVATION, PRIVACY AND CONSTITUTIONAL RIGHTS

Ekta Devi, LLM, Rayat Bahra University, Mohali, Punjab

ABSTRACT

Governance; financial transactions and public services have been transformed in' India by Digital Public Infrastructure (DPI). The' platforms like Unique Identification Authority of India Aadhaar; National Payments Corporation of India UPI; and Digi Locker have led to' greater efficiency; better access to' welfare schemes and digital inclusion. These systems have also contributed to' the' economic growth by speeding up services; eliminating the' use of paper and making the' services available to' the' nation's citizens easily. Simultaneously; a surge in' digital infrastructure has given rise to' significant legal and constitutional concerns to' privacy; data protection; exclusion of people and exclusion due to' technological barriers; as well as surveillance and cyber security.

Digital public infrastructure has brought up a host of legal issues in' India; which are explored in' this paper through a study of the' constitutional provisions; statutes and judicial pronouncements related to' Aadhaar; UPI and Digi Locker. The' study explores the' significance of the' right to' privacy in' light of Article 21 of the' Indian Constitution and examines the' ways in' which the' courts have been dealing with issues of informational privacy and state interference in' personal data. The' paper also examines the' relevance of the' laws like the' Information Technology Act; 2000 and the' Digital Personal Data Protection Act; 2023 in' relation to' regulation of digital systems.

The' paper proposes that the' technological innovation should be combined with constitutional protection of the' individual rights and democratic values. It finds that there is a need for more robust accountability mechanisms; clear regulatory frameworks and effective data protection in' India to' ensure that digital development does not erode constitutional freedoms.

Keywords: Digital Public Infrastructure; Aadhaar; UPI; Digi Locker; Privacy; Constitutional Rights; Data Protection; Digital Governance.

➢ Introduction

The' digital revolution and online public service delivery systems have brought a significant change in' governance in' India. Digital technology and online public service delivery systems have ushered in' a change in' governance in' India. Digital Public Infrastructure (DPI) is an emerging model where the' government provides services; runs identification systems; processes official payments through the' digital system; and keeps official records digitally. Aadhaar; UPI and Digi Locker have become a part of the' citizen's daily life and has transformed the' citizen-State relationship as a whole. Today; these systems are used in' a wide variety of fields; including banking; welfare; identity verification; education; health care; and tax administration and administration. The' growth of digital infrastructure is a testament to' India's efforts to' establish a new governance paradigm that leverages technology to' meet the' needs of a vast and diverse population more effectively and efficiently[1].

The' launch of Aadhaar was a milestone in' India's efforts to' embrace digital governance. Aadhaar was conceived as a biometric identity system to' be provided to' every citizen with a unique identification number and biometric and demographic details. Aadhaar was eventually equated with welfare schemes; banking service; mobile verification; public distribution system. The' government in' its eyes saw Aadhaar as a tool to' curb corruption; eradicate duplicate identities and to' make benefits reach the' citizens directly. In' the' meantime there was a growing concern about the' collection and storage of personal data that is sensitive and private; the' potential for misuse of biometric data and the' possibility of constant monitoring by the' State. The' controversy over Aadhaar slowly morphed into' a bigger debate on constitution; privacy; dignity and informational autonomy[2]. Another major contributor to' the' digital transformation of India was the' Unified Payments Interface (UPI). The' Unified Payments Interface (UPI) was also a significant factor in' the' digital transformation of India; by revolutionizing the' way financial transactions are conducted. UPI made it possible to' transfer money instantly via the' mobile app and made digital payments easy for citizens; businesses and the' government. The' platform has helped in' the' path towards cashless economy and increase the' use of digital transactions. It was in' the' urban and rural areas that small traders; street vendors; and consumers increasingly started to' use online payment systems. Despite these advantages; there were legal concerns related to' cyber security risk; financial fraud;

[1] R. Ramakumar, *Digital India and the Transformation of Governance*, 54 Econ. & Pol. Wkly. 23 (2019).
[2] Usha Ramanathan, *Aadhaar: From Welfare to Surveillance*, 26 Econ. & Pol. Wkly. 35 (2014).

financial data tracking and security of financial data associated with the' rise of digital payments revolution. With the' expansion and adoption of digital payment systems across the' country; concerns were raised regarding liability; accountability; and regulation[3]. Another significant aspect of India's Digital Public Infrastructure is Digi Locker; which facilitates paperless governance and ensures the' secure storage of official documents digitally. The' citizens are now able to' download their educational certificates; identity records; driving licenses and necessary documents from online platforms. This system reduced the' use of physical paper; and improved administration in' public and private sectors. However; problems like data security; unauthorized access and digital exclusion were still a significant concern regarding Digi Locker. Equality and accessibility[4] are issues with digital governance and the' use of such services where citizens lack access to' the' internet and/or are not techno literate.

However; in' today's India; its definition has also changed due to' the' increased dependence on digital systems. Digital platforms are not only changing the' nature of decision-making and service delivery but also the' ways in' which citizens are engaged and how financial inclusion is being realized; making public administration out of the' box of traditional administrative procedures. Digital governance has helped to' bring transparency in' many fields and has cut down on the' delays in' administrative functions. Digitalization has also driven economic development and technological innovation with government measures to' support it. But there are constitutional and legal issues that can't be brushed aside with this change. The' collection of large amounts of personal data by public bodies raises significant issues around privacy; surveillance and the' misuse of information. In' a democratic society where protection of the' freedoms of the' individual is the' cornerstone of democratic government; these concerns are heightened.

The' Supreme Court; in' its case of Justice K.S. Puttaswamy vs Union of India; declared the' right to' privacy as a fundamental right with Article 21 of the' Constitution. The' judgment highlighted the' close connection between privacy and human dignity; autonomy and freedom. It also emphasized the' importance of a balance between technological progress and constitutional protection. The' ruling had an impact on the' ongoing discussions about Aadhaar; digital data gathering; and state surveillance[5]. Digital governance structures based on

[3] Prasanna S., *Digital Payments, Financial Inclusion and Regulatory Challenges in India*, 15 Indian J. L. & Tech. 67 (2021).
[4] Nikhil Dey & Aruna Roy, *Digital Governance and Social Exclusion in India*, 55 Econ. & Pol. Wkly. 18 (2020).
[5] Arghya Sengupta, *The Aadhaar Judgment and the Future of Privacy in India*, 12 NLSI Rev. 89 (2019).

the' Constitution have been subject to' debate in' a number of cases in' India; where the' issues raised relate to' conflicts with fundamental rights or unreasonable restrictions on freedom. Hence; the' interpretation by the' courts are now at the' very core of the' constitutional debate of Digital Public Infrastructure in'India.

The' aim of this paper is to' explore the' legal dimensions of Aadhaar; UPI; and Digi Locker under the' paradigms of constitutional law and digital governance. The' themes of privacy; cybersecurity; surveillance; data protection; accessibility and digital exclusion are explored. It also looks at whether current laws can safeguard citizens against the' misuse of personal information and overreach by the' state when it comes to' digital information. The' paper also delves into' the' implications of the' Information Technology Act; 2000 and Digital Personal Data Protection Act; 2023 in' regulating digital systems and holding the' governance mechanism accountable[6].

The' study also tries to' explore if India's rapidly growing Digital Public Infrastructure is operating in' synergy with constitutional principles of dignity; liberty; equality and informational privacy. The' focus lies on the' increasing conflicts between technological innovations and the' safeguarding of fundamental rights in' a digital society. There is also a focus on transparency; oversight; cyber security concerns and the' lack of adequate mechanisms to' prevent misuse of digital data. The' research draws on constitutional provisions; statute; judicial decisions; government reports and publications; academic writing; and scholarly commentary on digital governance and privacy law[7]. The' study adopts doctrinal-Analytical approach to' comprehend the' constitutional and legal aspects of Digital Public Infrastructure in India.

- **Constitutional and Legal Framework of Digital Public Infrastructure**

Digital Public Infrastructure in' India has reshaped governance and administration structures and public service provision. Technological innovation is no longer the' sole domain' of platforms like Aadhaar; UPI and Digi Locker; as they have become key technologies of governance and economic regulation. While these systems have proven effective in' distributing welfare; conducting financial transactions; and ensuring digital documentation;

[6] Rahul Matthan, *Data Protection and Governance in India*, 7 Indian J. L. & Tech. 101 (2018).
[7] Shreya Atrey, *Data Protection and Informational Privacy in India: Constitutional Perspectives after Puttaswamy*, 9 Indian J. Const. L. 112 (2020).

they have also sparked critical constitutional and legal issues related to' privacy; surveillance; accountability; and data security. India's constitutional structure significantly contributes to' the' legal and boundaries of digital governance mechanisms. Digital Public Infrastructure directly impacts the' way citizens interact with the' State; and constitutional values of dignity; liberty; equality; and privacy are key in' assessing how these systems operate[8]. While not explicitly mentioned in' the' Constitution of India; the' fundamental principles of the' Constitution of India form the' basis for regulating technological systems and the' informational privacy. The' India Constitution works on the' principles of democratic accountability; rule of law; protection of individual liberty and welfare administration. Digital governance is a contemporary manifestation of these constitutional aspirations due to' the' growing use of technology to' enhance access to' public services; financial inclusion and administrative transparency. The' efforts of the' government in' the' field of digitization are aimed at reducing corruption; making bureaucratic procedures easier; and empowering the' public in' governance. Digital has also reinforced the' concept of inclusive governance by providing citizens with the' possibility of availing of services without having to' cross any physical boundaries. Concurrently; constitutional issues emerge when digital systems grant the' government too much control over personal data; or offer inequitable access to' public services[9].

The' Constitution provides for equality before law and equal protection of laws in' Article 14. Digital governance mechanisms should therefore function in' a way that does not exclude those who are not digitally literate; do not have an internet connection or technological means. In' many instances; rural people; the' poor; the' elderly and the' marginalized are excluded; due to' technological constraints. There can be an indirect violation of the' principle of equality if citizens cannot avail welfare schemes or even important services due to' failure of authentication or technology infrastructure. A constitutional vision of digital governance thus needs to' take care of both efficiency and inclusiveness to' ensure that technological progress does not exacerbate social inequalities[10].

The' Constitution's Article 19 also comes into' play in' relation to' digital governance as freedom of speech; freedom of expression; freedom to' communication and freedom to' access information are all impacted by digital platforms. There is a vast amount of personal and

[8] Anup Surendranath, *Constitutionalism in the Age of Digital Governance*, 11 Indian J. Const. L. 71 (2018).
[9] Reetika Khera, *Aadhaar and the Right to Food*, 52 Econ. & Pol. Wkly. 50 (2017).
[10] Jean Drèze, *Technology, Welfare and Social Justice in India*, 53 Econ. & Pol. Wkly. 37 (2018).

behavioural data generated by online payment systems; electronic documentation and digital identification systems. State agencies or private parties using such information could also result in' restrictions on individual autonomy and freedom. If citizens have concerns about their personal data being constantly monitored or used improperly; they may be reluctant to' use their freedoms. This is an even greater worry in' a democratic society where constitutional freedoms are closely linked to' individual dignity and personal freedom[11].

The' interpretation of Article 21 of the' Constitution as granting the' right to' privacy was a major milestone in' Indian constitutional law. The' Supreme Court in' Justice K.S. Puttaswamy v. Union of India has ruled that privacy is integral to' the' right to' life and personal liberty. The' Court acknowledged bodily privacy; decisional autonomy; and informational privacy as all components of privacy. In' the' context of Digital Public Infrastructure; informational privacy gained special significance due to' the' large scale collection; storage and processing of personal information in' digital systems. The' judgment highlighted the' importance of balancing the' required restrictions with privacy rights; noting that any such restrictions must meet the' four-part test for legality; necessity; proportionality and procedural safeguards. This ruling set boundaries for state data collection and surveillance activities[12].

The' Aadhaar Act; 2016 was passed for the' purpose of giving statutory recognition to' the' Aadhaar identification system. The' Act empowers the' collection of biometric data and demographic data for giving unique identification numbers to' citizens of India. The' government's stance has been that Aadhaar is a good means of targeted delivery of welfare benefits and plugging leakages in' subsidy schemes. Slowly Aadhaar was linked to' banking; SIM card verification; taxation and public welfare schemes. The' Aadhaar system; although beneficial; faced significant legal challenges related to' privacy; data protection; and the' potential for state surveillance. Centralization of biometric data was criticized for the' danger of misuse of personal information; profiling of citizens and unauthorized access to' data stored in' a central repository[13].

The' validity of Aadhaar was contested in' the' Supreme Court in' K.S. Puttaswamy (Aadhaar-5J.) v. Union of India. The' Court declared the' Aadhaar scheme was constitutional but introduced some conditions on the' use of Aadhaar. While the' judgment said that Aadhaar

[11] Gautam Bhatia, *Privacy, Autonomy and Constitutional Rights*, 10 Indian J. Const. L. 29 (2017).
[12] B.B. Pande, *Privacy and Surveillance in Contemporary India*, 6 NUJS L. Rev. 201 (2015).
[13] Vrinda Bhandari, *Biometric Identification and Constitutional Freedoms*, 14 Indian J. L. & Tech. 82 (2019).

could be used for welfare purposes; it overturned law allowing private companies to' provide authentication services. The' Court stressed that the' State may not establish a system of surveillance which unduly interferes with the' privacy of individuals. It also emphasized the' need for data protection and consent on digital governance systems. Despite court review; there are still questions about the' security of biometric databases; exclusions due to' authentication errors; and the' level of access the' State has to' biometric information[14].

The' Reserve Bank of India (RBI) and the' National Payments Corporation of India (NPCI) are primarily responsible for overseeing the' regulatory framework of UPI and digital payment systems. UPI is one of the' most successful mobile applications that makes it possible to' do instant financial transactions; which is why it is one of the' most successful digital payment systems in' the' world. The' fast-growing digital payment system has fostered financial inclusion and boosted India's digital economy. In' recent years; online payment systems have become a critical part of the' way small businesses; consumers and public institutions transact every day. However; the' rise of digital payments has also brought with it worries about cybersecurity; financial fraud; unauthorized payments and financial data misuse[15].

RBI's role in' regulating payment systems and financial stability in' the' digital economy is significant. The' RBI has issued several regulations and circulars regarding data localization; consumer protection; and cybersecurity standards; as well as the' security of digital payments. NPCI; the' controlling body of the' operational structure of UPI; also helps in' the' development and supervision of the' payment infrastructure. Yet; phishing attacks; identity theft; hacking; and fraudulent transactions remain' a challenge to' the' effectiveness of the' governance of digital payments[16]. When users experience financial harm as a result of technological vulnerabilities or cybercrimes; questions of liability and accountability come up. Another significant part of India's Digital Public Infrastructure is Digi Locker. Digi Locker is part of the' Digital India initiative that enables citizens to' store and retrieve official documents digitally. The' educational certificates; licenses; identity cards; and other government documents are now available digitally without any physical documents. The' system enables a paper-free governance and streamlines the' administrative process in' different fields. Digi Locker is a part of the' overall e-governance policies and electronic record recognition under

[14] Arghya Sengupta, *Revisiting Aadhaar after Puttaswamy*, 13 NLSI Rev. 55 (2020).
[15] V. Balasubramaniyan, *Regulating Digital Payment Ecosystems in India*, 17 Indian J. L. & Tech. 143 (2022).
[16] Rohit Prasad, *Cybersecurity Challenges in India's Digital Economy*, 58 Econ. & Pol. Wkly. 41 (2023).

the' laws of India. The' growing use of electronic documents is as a result of the' State's efforts towards modernization of administrative systems and making them accessible to' the' public.

While Digi Locker offers convenience and efficiency; it also brings up legal issues concerning cybersecurity and data protection. Security risks; data breaches and misuse of personal documents continue to' be significant challenges in' electronic governance systems[17]. Digital documentation can also pose a challenge for citizens who are not technologically literate or don't have access to' the' internet. Thus; equal access to' public services is a relevant constitutional principle in' the' assessment of how digital documentation systems work.

The' cornerstone of the' Indian cyber law and e-communications are the' Information Technology Act; 2000. The' Act grants legal validity to' electronic records; digital signatures and electronic transactions. It also has provisions concerning cyber offences; hacking; identity theft; data breaches and unauthorized access to' computer systems. The' Information Technology Act has played a significant role in' facilitating Digital governance by providing a legal framework for Electronic Commerce and Digital Administration. The' provisions on intermediary liability; cybersecurity obligations and electronic authentication continue to' have an impact on the' working of Digital Public Infrastructure in' India.

The' Information Technology Act; however; has been subject to' many criticisms for failing to' properly account for modern issues related to' artificial intelligence; mass surveillance; and massive data processing. The' law under the' Act has lagged behind technological advancements. There have been ongoing concerns about issues of enforcement; inadequate privacy protections; and insufficient safeguards for misuse of personal data. Such restrictions made it more imperative to' have a special data protection legislation which is better able to' govern data practices in' the' digital world[18].

The' Digital Personal Data Protection Act; 2023 (the' Act) is introduced as a law on the' processing and protection of personal data in' India. The' Act is about the' right of individuals to' have control over their own data and the' duties of organisations that hold digital data. It introduces the' notions of consent-based data processing; lawful use of personal information; data security requirements and grievance redressal mechanisms. The' bill strives to' strike a balance between innovation and economic growth and the' protection of individual privacy

[17] Pavan Duggal, *Cyber Law and Electronic Governance in India*, 5 Indian J. Cyber L. 14 (2018).
[18] Sunil Abraham, *Data Governance and Privacy Regulation in India*, 9 Indian J. L. & Tech. 119 (2021).

rights. While the' Digital Personal Data Protection Act is a step towards regulating privacy; there are still some issues with the' wide-ranging exemptions for the' State and potential for too much governmental oversight over digital data. Some criticise the' Act for lacking adequate protections against the' state surveillance or arbitrary access to' personal data. There have also been some questions about the' autonomy of regulatory bodies and effectiveness of enforcement. The' implementation of the' legislation will thus be a key element to' the' success of upholding privacy rights in' India's growing digital government[19].

The' regulation and management of Digital Public Infrastructure (DPI) in' India is a critical role played by several institutions. The' Aadhaar system and the' management of biometric identification processes are handled by the' Unique Identification Authority of India (UIDAI). The' Reserve Bank of India is the' regulator of digital payments and financial technology. The' National Payments Corporation of India regulates the' infrastructure and electronic transaction methods of UPI. The' Ministry of Electronics and Information Technology (MeitY) formulates policies related to' digital governance; cyber security and electronic administration. All these institutions; together; contribute to' the' legal and administrative framework of digital governance in' India. As technology is more embedded in' governance; Digital Public Infrastructure is closely tied to' constitutional rights and democratic accountability. Digital systems have brought efficiency; accessibility and innovation; but also new legal issues concerning privacy; surveillance; exclusion and cyber security. The' constitutional and legal framework for these systems should therefore guarantee that technological advances do not restrict the' individual freedoms or the' principles of democracy.

- **Judicial Interpretation and Case Law Analysis**

Justice K.S. Puttaswamy v. Union of India: Right to' Privacy

The' case of Justice K.S. Puttaswamy vs Union of India (2017) is a landmark decision in' Indian constitutional law as it established the' right to' privacy as a fundamental right under Article 21 of the' Indian Constitution. A nine-judge constitutional bench unanimously held that privacy is an essential part of the' right to' life and personal liberty. The' Court noted the' close link between privacy and dignity; autonomy; liberty; and individual freedom[20]. This ruling has had a major impact on the' legal landscape of Digital Public Infrastructure in' India; given that

[19] Mishi Choudhary, *Digital Rights and Data Protection in India*, 16 Indian J. L. & Tech. 91 (2023).
[20] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

digital platforms like Aadhaar; UPI; and Digi Locker require the' collection and processing of vast amounts of personal data. The' Court explained that informational privacy plays an essential part in' the' protection of the' constitution in' a digital society. It understood that technological advances have enhanced the' capabilities of the' State and of private organisations to' gather; monitor and analyse personal data. The' judgment pointed out that unrestricted data collection can amount to' a surveillance universe with the' potential to' endanger democratic freedoms. The' Court also found that any interference with the' right to' privacy has to' meet the' tests of legality; necessity; proportionality and procedural safeguards. This principle set constitutional boundaries to' state interference in' personal data or digital governance systems[21].

The' dangers of profiling and misuse of digital information were also discussed in' the' judgment. The' Court noted that digital records can contain' very private information about an individual's identity; financial habits; health and social interactions. This determined the' constitutional basis for assessing the' legality of Aadhaar authentication; digital payments and e-governance processes in' the' context of Digital Public Infrastructure. Thus; privacy came to' be recognised as a fundamental right; thereby changing the' whole debate on data protection and state surveillance in' India[22].

Constitutional Validity of Aadhaar Scheme

In' K.S. Puttaswamy (Aadhaar-5J.) v. Union of India (2018); the' constitutionality of the' Aadhaar scheme was challenged. Aadhaar project was launched under Aadhaar Act; 2016 with an aim of creating an indigenously biometric identity system for the' people of India. The' scheme required individuals to' submit biometric and demographic information for obtaining a unique identification number. The' government pointed out that Aadhaar would make welfare distribution more effective; curb corruption and weed out ghost beneficiaries from subsidy programmes[23].

The' petitioners challenged the' Aadhaar scheme on various constitutional arguments such as violation of privacy; mass surveillance; data insecurity; and exclusion from welfare benefits due to' failure to' authenticate. There were also concerns about the' centralization of the'

[21] Gautam Bhatia, *Privacy, Autonomy and Constitutional Rights*, 10 Indian J. Const. L. 29 (2017).
[22] Apar Gupta & Nikhil Pahwa, *Privacy and the Indian Constitution in the Digital Age*, 8 Indian J. Const. L. 45 (2015).
[23] Usha Ramanathan, *Aadhaar: From Welfare to Surveillance*, 26 Econ. & Pol. Wkly. 35 (2014).

biometric data and the' potential for misuse by government institutions or private companies. The' Supreme Court gave a nod of approval to' the' constitutionality of Aadhaar by a majority vote with important caveats[24].

The' Court opined that the' use of Aadhaar for welfare programmes and public subsidies falls within' the' ambit of a legitimate state interest as it helps in' efficient delivery of welfare programmes. Meanwhile; the' Court also invalidate Section 57 of the' Aadhaar Act that permitted private companies to' avail Aadhaar authentication services. The' judgment pointed out that biometric data may not be allowed unrestricted access by private organizations since it may have serious consequences on informational privacy. The' Court also stated that Aadhaar cannot be made compulsory for services like verification of mobile SIMs and school admissions.

The' ruling was the' courts' effort to' reconcile technological advancements and constitutional rights. The' Court upheld the' utility of Aadhaar in' the' digital governance sector and also acknowledged the' risks of surveillance and misuse of Aadhaar data. Some critics of the' judgment contended that it failed to' take into' account any of the' concern about the' centralization of data and state control of biometric databases. Despite the' courts' attention; questions have been raised about data protection; rights of exclusion due to' authentication failure; and the' possible long-term constitutional consequences of biometric governance.

Judicial Approach towards Surveillance and Data Collection

Indian courts have had a long discussion on the' topics of surveillance; interception of communications; and monitoring of personal information done by the' state. There is increasing judicial concern about over-assertive states and techno-intrusions into' private life in' this area. The' Supreme Court in' People's Union for Civil Liberties (PUCL) v. Union of India (1997) dealt with the' issue of legality of telephone tapping under the' Indian Telegraph Act; 1885. The' Court ruled that the' use of the' intercepting devices to' listen to' his calls without his consent is a violation of his right to' privacy under Article 21. It also put into' place procedural safeguards for telephone surveillance and reinforced that powers of surveillance must not work without legal restrictions[25].

[24] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.
[25] Arghya Sengupta, *The Aadhaar Judgment and the Future of Privacy in India*, 12 NLSI Rev. 89 (2019).

Later; in' the' digital age in' which governments have much more technological power to' monitor citizens; the' principles set forth in' the' PUCL judgment were relevant. The' use of the' modern surveillance tools like the' biometric database; facial recognition technology; and digital tracking has sparked significant constitutional issues. The' courts have increasingly recognized that digital surveillance can have chilling effects for freedom of speech; political engagement and/or personal freedom.

In' Anuradha Bhasin' v. Union of India (2020); the' Supreme Court had considered the' restrictions placed on the' internet in' Jammu and Kashmir. The' Court held that the' use of the' Internet is in' close proximity to' freedom of speech and expression protected under Article 19(1)(a). The' case had a focus on proportionality in' relation to' restrictions on digital communication. While the' case was mainly about the' internet shutdowns; it illustrated a judicial understanding of how closely digital technologies are intertwined with constitutional freedoms[26].

The' concern of judges about surveillance is also featured in' discussions on spyware technologies like Pegasus. The' Supreme Court had appointed an expert committee to' look into' complaints of spyware usage for unauthorized surveillance of journalists; activists and public figures in' the' case of Manohar Lal Sharma vs Union of India (Pegasus Case; 2021). The' Court noticed that national security cannot be an umbrella cover for the' violation of the' right to' the' Constitution. The' judgment marked the' growing awareness of the' Judiciary to' the' potential risks of cutting-edge digital surveillance technologies[27].

Informational Privacy and Fundamental Rights

In' the' digital era; the' right to' informational privacy has become a key constitutional concern; as much of governance is dependent on data collection and the' use of digital identification. In' Justice K.S. Puttaswamy v. Union of India; the' Supreme Court found that; informational privacy is an integral aspect of freedom of the' person. The' judgment made clear that people have to' have control over how their personal data is disseminated and used. This concept has a direct impact on Digital Public Infrastructure as large amounts of sensitive personal information are gathered by systems like Aadhaar and Digi Locker.

[26] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[27] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

The' Court noted that informational privacy is the' right to' the' non-disclosure of information; as well as the' right to' protection against misuse; profiling and exploitation. In' digital governance systems; citizens are often required to' share biometric details; financial information; and identity records for accessing public services. If there is no appropriate safeguarding; people may be at risk of surveillance; discrimination and identity theft. The' judicial interpretation has; therefore; more and more shifted its attention to' the' balance between the' administrative efficiency and the' protection of the' constitutional freedoms[28].

The' right to' informational privacy is also related to' Article 19 and Article 14 of the' Constitution. The' risk of over-collection of personal data can have an indirect effect on freedom of speech and expression as people may be afraid of being continuously monitored. In' the' same way; discriminatory use of digital data could be contrary to' the' constitutional protection for equality before the' law. Thus; the' courts have highlighted transparency; consent; and accountability in' the' system of digital governance. The' recent Digital Personal Data Protection Act; 2023 is another testament to' the' increasing legalization of informational privacy in' India. The' law seeks to' control digital data processing; but the' government has large exemptions. The' law's ability to' account for constitutional rights in' the' digital world will likely be decided by judicial review in' future cases[29].

Judicial Concerns regarding Digital Exclusion

Digital exclusion in' welfare administration and public services; due to' technological dependence; has also been a subject of discussion in' Indian courts. Although the' goal of Digital Public Infrastructure is to' make things more efficient and accessible; there are technological hurdles that are difficult for economically weaker and marginalized communities. Many people have been denied welfare benefits due to' authentication failures; no access to' internet; technical failures; or lack of digital literacy.

In' Swaraj Abhiyan v. Union of India (2016); the' Supreme Court emphasized that the' delivery of food security schemes must be kept free of procedural requirements that prevent vulnerable people from getting the' benefits of such schemes. Though this was not directly related to' Aadhaar; subsequent judicial debates related to' the' exclusion of welfare to' technological

[28] Manohar Lal Sharma v. Union of India, W.P. (C) No. 314 of 2021 (Pegasus Case).
[29] Shreya Atrey, *Data Protection and Informational Privacy in India: Constitutional Perspectives after Puttaswamy*, 9 Indian J. Const. L. 112 (2020).

authentication failures. There have been concerns raised by several High Courts in' India about denial of ration benefits caused by mismatch in' biometric systems.

The' Jharkhand starvation death cases were given national attention as there were reports that despite the' authentication issues of Aadhaar; food to' the' beneficiaries was denied. This sparked legal arguments about the' constitutionality of requiring mandatory BV for welfare access[30]. Courts noted that no consideration could be given to' the' administrative efficiency over the' right to' life under Article 21. It is thus important that welfare systems will be available even if digital technology breaks down. In' Faheema Shirin' v. State of Kerala (2019); the' Kerala High Court has held that the' right to' access internet is a part of right to' education and privacy in' Article 21 of the' Constitution. The' judgment recognized that digital access is a crucial component of engagement in' today's society[31]. This consideration was especially relevant to' the' sense of the' potential impact of digital exclusion on constitutional rights within' a governance regime that is increasingly digital.

Cybersecurity; Digital Fraud; and Judicial Responses

Along with the' booming expansion of Digital Public Infrastructure; cybersecurity breaches; online fraud; identity theft; and unauthorized use of personal information also have surged. Indian judiciary is repeating the' need for safeguarding digital systems from cyber attacks. In' India; the' main' piece of legislation which governs cyber offenses is the' Information Technology Act; 2000. Electronic and hacking; identity theft; and cheating through electronic means are all common topics that are often referenced in' digital fraud situations. The' Supreme Court in' Shreya Singhal v. Union of India (2015) invalidated Section 66A of the' Information Technology Act as being a violation of freedom of speech and expression as guaranteed by Article 19(1)(a). While the' case was mostly about online expression; the' judgment echoed the' courts' worries about the' abuse of digital regulatory authority. The' Court emphasized that vague and excessive restrictions in' cyber laws may threaten constitutional liberties[32].

Digital payment systems have also brought in' cases of banking fraud; phishing attacks; and unauthorized electronic transactions which have been addressed by the' Indian courts. The' RBI has come out with consumer protection guidelines; which have made banks and payment

[30] Rahul Matthan, *Data Protection and Governance in India*, 7 Indian J. L. & Tech. 101 (2018).
[31] Swaraj Abhiyan v. Union of India, (2016) 7 SCC 498.
[32] Faheema Shirin R.K. v. State of Kerala, 2019 SCC OnLine Ker 1733.

service providers liable in' the' event of unauthorised transactions. Judicial fora such as consumer courts and High Courts have been increasingly acknowledging the' importance of financial institutions building a robust cybersecurity regime to' ensure the' safety of customer information.

The' growing reliance on Aadhaar-based databases and online payment platforms has elevated the' significance of cybersecurity matters. Legal issues have been under scrutiny several times after the' unauthorized exposure of Aadhaar data in' various breaches of data security; considering a centralized digital database. Encryption; data minimization; and cybersecurity measures have been emphasized as key components in' safeguarding sensitive personal information. The' interpretations in' the' judicial sphere have demonstrated the' realization of the' need to' have legal protections to' combat and prevent cyber threats and the' misuse of digital information in' order to' have a proper functioning of the' systems of digital governance. Courts will have an important role to' play as India continues to' build out Digital Public Infrastructure (DPI) to' ensure that technological evolution aligns with constitutional rights; democratic accountability and safeguarding of individual freedoms[33].

- **Challenges and Constitutional Concerns in' Digital Public Infrastructure**

Digital Public Infrastructure in' India; while contributing to' technological advancement and administrative efficiency; raises significant constitutional and legal concerns due to' its rapid growth. The' possibilities of large scale intrusions into' personal privacy have emerged in' the' governance and public service delivery system through platforms like Aadhaar; UPI; and Digi Locker. With the' data collected; stored and processed in' these systems; surveillance and misuse of information has become the' centre of the' constitutional debates in' India. The' State now has unparalleled access to' citizen biometric data; the' details of their financial transactions; their identities and their behaviours. This aggregation of data has raised concerns that over time; digital governance systems could evolve into' regimes of mass surveillance that track individuals' behaviors without the' necessary legal protections.

Given the' nature of digital systems; and the' possibility of continuous tracking and profiling of individuals through interconnected databases; the' concern is elevated. As a whole; Aadhaar authentication; the' documentation of digital payments and online documentation systems

[33] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

produce a whole lot of personal data that can indicate financial patterns; social behaviour; and movement. If no restrictions are put in' place; such information could be used for profiling; tracking dissent or access control for public facilities. The' right to' privacy in' Article 21 demands that interference by the' State in' private life has to' be limited; proportionate and lawful. Too much surveillance is a threat to' democracy; as citizens can grow to' fear the' constant observation of the' authorities. This environment can have indirect effects on limiting freedom of speech; political participation and individual autonomy in' a constitutional democracy.

Another key challenge to' Digital Public Infrastructure is data breaches and cyber threats. With the' growing reliance of India on digital platforms for governance and financial transactions; the' likelihood of hacking; unauthorized access; and leakage of sensitive data has grown more and more extensive. With a number of reports about the' leakage of Aadhaar related data and online financial fraud; questions have emerged about the' security of centralized digital databases. Payment systems; banking applications and electronic identity records are all common targets of cybercriminals for financial gain' and for obtaining identities. This is because; unlike passwords; biometric data cannot easily be replaced once leaked or hacked; and there are other risks as well from the' large-scale storage of biometric information[34].

The' upsurge in' cyberattacks is proof that technological development without effective security systems could put citizens at great risk. Many users of digital systems are unaware of online fraud; phishing attacks and cybersecurity; making them more susceptible to' exploitation. Unauthorised UPI transactions leading to' financial fraud are becoming common among both urban and rural people. Although there are regulations like the' Reserve Bank of India and the' Ministry of Electronics and Information Technology's cybersecurity guidelines; there are issues with poor enforcement and slow response to' data breaches. The' guarantee of the' State in' the' constitution to' safeguard the' life and personal liberty of its citizens also encompasses the' duty to' ensure that citizens' personal information is safeguarded within' the' digital governance system.

Digital Public Infrastructure has also worsened the' issue digital divide and technological exclusion. Despite the' goals of digital governance which are to' increase accessibility and efficiency; many citizens do not have access to' the' internet; smartphones; digital literacy; or

[34] Rohit Prasad, *Cybersecurity Challenges in India's Digital Economy*, 58 Econ. & Pol. Wkly. 41 (2023).

technological resources to' access digital governance systems. People in' rural areas; elderly; and the' disabled and economically weaker sections of the' society may have challenges to' avail online services. This reliance on digital platforms can thus indirectly create a form of discrimination for vulnerable populations with regard to' access to' welfare schemes; banking services; healthcare and education.

The' risks of exclusion due to' technological dependence have been further accentuated by authentication failures under Aadhaar-linked welfare systems. Denial of ration supply or welfare benefits on the' ground of mismatch of biometric data has led to' serious constitutional questions of right to' life as stated in' Article 21. Digital systems are increasingly used to' govern and citizens who are not able to' use them can effectively be cut off from governance processes. The' fundamental value of equality guaranteed by Article 14 of the' Constitution must be observed in' the' system of governance so that it is accessible to' every segment of society regardless of technological competence. Leaving out the' marginalized and underserved communities in' a governance framework that serves the' digitally privileged can worsen social and economic inequities. An additional major constitutional issue is the' consent and data sharing policies of Digital Public Infrastructure. In' many cases; citizens have to' give their private information to' access basic services through digital governance systems. In' many instances; people don't have a lot of understanding of how their data is collected; processed; stored or shared with various agencies. In' digital systems; consent can be tokenistic as users might not have a meaningful choice in' accepting terms and conditions. This raises issues about informational autonomy and personal control over personal data.

Data sharing among the' different departments of the' government and private companies contributes to' the' possibility of misuse and unauthorized access. In' large-scale integration; when databases are used; environments are created where sensitive personal data is exchanged without transparency or accountability. Citizens may not know just how much their financial information; biometric data or behavioural data is being tracked or studied. This undermines the' constitutional guarantee of privacy and can lead to' arbitrary interference in' people's lives. The' Digital Personal Data Protection Act; 2023 aims to' govern data processing and consent procedures; but issues remain' about the' wide exemptions granted to' government agencies and the' lack of real oversight for individuals over their data.

The' lack of transparency and accountability also poses huge legal and constitutional issues in' the' digital governance framework. The' working of Digital Public Infrastructure involves complex technological systems which are currently being overseen by various regulatory institutions such as UIDAI; RBI; NPCI; and MeitY. People in' the' street are not always clear about how these systems work; who's accountable when things go wrong; or when there's a technological malfunction. Algorithmic decision-making processes may be hidden in' digital systems and are thus not subject to' public review; leaving little room to' contest errors and discriminatory results.

Lack of transparency is especially problematic when citizens are losing out financially; are denied benefits to' which they are entitled; or privacy is violated. Mechanisms of accountability in' digital governance settings are still developing; and legal action may be delayed or ineffective. It is often a challenge for data breach and digital fraud victims to' obtain' damages or enforce their rights. However; lack of independent oversight institutions that are able to' hold digital governance systems effectively to' account undermines public trust; and could lead to' concerns about power concentration within' the' executive. The' need to' balance technological innovation with constitutional guarantees is thus one of the' most crucial challenges of Digital Public Infrastructure in' India. Digital systems have undoubtedly made it more efficient; more transparent and more financially inclusive; but constitutional democracy must always ensure that technological progress does not sacrifice individual freedoms and human dignity. Unfettered collection of information about individual people or establishment of structures of governance that are focused on surveillance cannot be justified by innovation. In' a technology-oriented society; constitutional rights have to' continue to' be respected; including privacy; equality; liberty and freedom of expression.

The' challenge is creating a rulebook that can foster digital innovation without exposing citizens to' misuse of power and techno-exploitation. In' order to' achieve a constitutional balance; stronger cybersecurity protections; data governance practices that are transparent and understandable; meaningful consent mechanisms; and independent regulatory oversight are necessary. The' interpretation of the' judiciary will also have a significant role to' play in' ensuring that Digital Public Infrastructure operates within' constitutional boundaries. The' future of democratic governance in' India will greatly depend on how technological advancement can coexist with constitutional morality; accountability and protection of fundamental rights.

- **Recommendations and Policy Reforms**

Digital Public Infrastructure (DPI) is a new opportunity in' governance; financial inclusion; and public service delivery in' India because of its fast development. Administrative efficiency and accessibility of various government services has been improved with the' implementation of platforms like Aadhaar; UPI; Digi Locker etc. Meanwhile; there has been a significant growth of digital systems which has brought with it vulnerabilities in' relation to' data protection; cyber security; accountability and constitutional guarantees. This is a reason why more policy reforms are required that can not only ensure citizens' rights but also enable technological innovation to' occur in' an equitable and democratic way.

The' security and reliability of data protection systems are of great importance to' ensure public confidence in' digital governance systems. India's Digital Personal Data Protection Act; 2023; is a crucial legislative measure to' govern the' handling of personal information; but there are still some areas that need to' be addressed. The' law should offer more protection for the' misuse of private information and for surveillance carried out by either public officials or private individuals. Data minimization; purpose limitation; storage limitation; informed consent should be given more emphasis. Citizens should have more control over their personal information by having the' right to' access; correct and delete their information wherever needed. In' addition; there should be significant fines for data breaches; for releasing confidential information without authorization or for misusing confidential information. Digital Public Infrastructure is highly dependent on the' use of biometric and financial information; and enhanced legal safeguards are required to' maintain' privacy and informational independence.

Emerging digital governance systems and their influence also raise the' need for independent regulatory oversight mechanisms. At present; various institutions like UIDAI; RBI; NPCI and MeitY have important administrative and regulatory powers but there are concerns of power concentration and external accountability. Independent oversight mechanisms not subject to' executive interference are required for oversight and adherence to' constitutional standards for digital systems. These institutions should have the' power to' investigate complaints of issues with privacy violations; surveillance practices; cybersecurity failures; and denial of digital services. Independent regulatory authorities would also boost public trust in' that governance is transparent; impartial and accountable. Technical expertise; legal professionals;

cybersecurity experts and civil society representatives should be part of oversight institutions; ensuring balanced decision-making.

The' constitutional right to' know how personal information is being collected; processed; stored and shared by citizens must be a key principle in' Digital Public Infrastructure. There are many digital systems that currently exist that have complex technological processes that are difficult to' understand for everyday people. A lack of transparency undermines public trust; and hampers the' potential for power to' be abused. Therefore; it is essential for government authorities and digital service providers to' provide transparent information on data usage policies; storage practices; surveillance mechanisms; and grievance redressal procedures. When the' information is passed on to' third parties or when it is used in' other ways than was originally created for; citizens have to' be notified.

Digital administration systems based on algorithms should also be subject to' public debate and judicial examination. Sometimes; automated decision-making processes can result in' discriminatory or arbitrary decisions regarding access to' welfare services; banking facilities; or public services. To' safeguard constitutional rights; the' transparent mechanisms for auditing digital systems and challenging administrative decisions are therefore necessary. Public accountability can also be enhanced by regular publications of transparency reports; cybersecurity audits and independent performance evaluations concerning Digital Public Infrastructure.

Inclusive and accessible digital systems for all segments of society are also a prerequisite for the' success of digital governance. Many citizens in' India are not connected to' the' Internet; do not own smartphones; and do not have access to' technological resources; which means that there is a significant digital divide. This can inadvertently leave out the' poor; the' rural population; the' elderly and people with disabilities from accessing public services which are vital to' them. The' constitutional commitment of equality as part of Article 14 entails governance systems are non-discriminatory and available to' vulnerable communities.

The' Digital Public Infrastructure must therefore focus on the' rights and inclusive aspects rather than the' technological aspects; keeping accessibility in' mind. There must be offline options and manual grievance procedures; as well; for those who are not able to' use digital platforms. All government policies should target to' increase internet access in' rural communities; enhance digital education initiatives; and create digital interfaces that are able

to' communicate with various user groups. Technological systems also need to' be designed to' be accessible to' people with disabilities and those who are not used to' working with digital systems. A rights-based approach to' digital governance could make sure that innovation is used to' enhance; not further exacerbate; social exclusion.

Reforms in' cybersecurity are also crucial; as Digital Public Infrastructure is growingly dealing with financial; personal; and biometric data. As cyberattacks; phishing schemes; data breaches; and cyber fraud increase; it becomes clear that current digital systems are not secure. Thus; an improved cybersecurity infrastructure is needed to' safeguard citizens from unauthorized access; identity theft; and financial exploitation. Implementing advanced encryption techniques; multi-factor authentication; and frequent security assessments for sensitive data is crucial for government agencies and digital payment platforms.

There is also a need for institutional changes to' enhance the' coordination between the' cybersecurity and the' digital governance regulatory bodies. Cybersecurity response teams should be established to' respond to' and contain' digital threats in' real time. The' departments of police; security; and law enforcement in' general; need upgraded technical training to' effectively address cybercrimes related to' the' digital payment systems and data theft. Public Awareness campaigns about internet fraud; internet security and safe internet practices should also be increased to' keep citizens safe from technological exploitation.

The' future of Digital Public Infrastructure in' India is hinged on the' capacity of the' legal system to' strike a balance between innovation and constitutional morality; and democratic accountability. Technological progress must not be allowed to' undermine the' privacy; liberty; equality or human dignity. Robust laws; clear governance; an inclusive cyber policy; and high-quality cyber-security are crucial to' keep digital transformation within' constitutional bounds. A democratic digital governance framework thus needs to' make citizens' rights the' focus of technological development; and not use efficiency as the' only aim of modernization.

- **Conclusion**

In' India; Digital Public Infrastructure is a significant enabler of governance and economic development. Digital platforms like Aadhaar; UPI and Digi locker have revolutionised public service provision; financial transactions and digital governance; boosting efficiency; accessibility and transparency. These systems have enhanced financial inclusion; made welfare

easier to' distribute; facilitated paperless governance and spread the' use of digital technology throughout society. The' increasing pace of digital governance shows India's effort to' create a technology-driven governance system that can effectively address the' needs of its vast population in' a modern and efficient manner.

In' parallel; the' study warns that the' scale of Digital Public Infrastructure has raised significant constitutional and legal issues of privacy; surveillance; cybersecurity; data protection and digital exclusion. Digital platforms collecting and holding biometric; financial and personal data raise the' potential for abuse of information; and for citizens to' be monitored without their knowledge. The' landmark judgments; like Justice K.S. Puttaswamy v. Union of India; have helped in' the' formalization of privacy as a fundamental right and laid a foundation for the' constitutional restrictions on the' State's involvement in' personal information. This decision in' the' Aadhaar case also highlighted the' judiciary's efforts to' reconcile welfare policies with the' protection of informational privacy and individual liberty.

The' study also finds that technological developments still pose some challenges with regard to' differential access to' digital systems in' India. Many people in' the' country remain' unconnected to' the' internet; lack digital literacy and have little or no technological or operational equipment to' be effective in' digital governance. Weaknesses in' the' current digital infrastructure can be seen in' authentication failures; cybersecurity threats and online financial fraud. While the' Information Technology Act; 2000 and Digital Personal Data Protection Act; 2023 provide frameworks to' regulate digital systems and safeguard personal information; there are concerns about implementation; transparency; and accountability measures.

Therefore; the' future of Digital Public Infrastructure in' India will significantly be hinged on the' existence of technological development with constitutional morality and democratic values. Digital innovation will fail if citizens don't have confidence that their personal information is secure and not being arbitrarily used. This means that a rights-based approach to' digital governance is required to' maintain' public trust; while avoiding the' constitutional freedom being undermined by the' modernisation. Data protection regulations; regulatory independence; clear governance procedures and robust cyber security protocols are key elements that will influence the' trajectory of India's digital governance model.

The' study further shows that the' technological efficiency cannot be the' main' goal of governance in' a constitutional democracy. Digital systems need to' be held accountable and accessible and inclusive to' all parts of society. No citizen must be deprived of welfare benefits; financial services or public opportunities for technological reasons or due to' being 'left behind' in' the' digital world. Digital governance mechanisms need to' continue to' be governed by constitutional principles; including dignity; equality; liberty; and privacy. While India's Digital Public Infrastructure has tremendous potential for enhancing governance and economic development; it must be balanced with innovation and constitutional rights for long term legitimacy. Digital governance's success will ultimately be judged not just by technological progress; but also by its ability to' defend and safeguard democratic values; individual freedoms and human dignity in' a more and more digital society.

References

- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
- Apar Gupta & Nikhil Pahwa, *Privacy and the Indian Constitution in the Digital Age*, 8 Indian J. Const. L. 45 (2015).
- Arghya Sengupta, *The Aadhaar Judgment and the Future of Privacy in India*, 12 NLSI Rev. 89 (2019).
- Faheema Shirin R.K. v. State of Kerala, 2019 SCC OnLine Ker 1733.
- Gautam Bhatia, *Privacy, Autonomy and Constitutional Rights*, 10 Indian J. Const. L. 29 (2017).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.
- Manohar Lal Sharma v. Union of India, W.P. (C) No. 314 of 2021.
- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- Rahul Matthan, *Data Protection and Governance in India*, 7 Indian J. L. & Tech. 101 (2018).
- Rohit Prasad, *Cybersecurity Challenges in India's Digital Economy*, 58 Econ. & Pol. Wkly. 41 (2023).
- Shreya Atrey, *Data Protection and Informational Privacy in India: Constitutional Perspectives after Puttaswamy*, 9 Indian J. Const. L. 112 (2020).
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- Swaraj Abhiyan v. Union of India, (2016) 7 SCC 498.
- Usha Ramanathan, *Aadhaar: From Welfare to Surveillance*, 26 Econ. & Pol. Wkly. 35 (2014).