INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

RESEARCH PAPER ON DIGI-LOCKER AS A TOOL OF DIGITAL GOVERNANCE: BALANCING EFFICIENCY, PRIVACY, AND ACCOUNTABILITY IN DELEGATED LEGISLATION

AUTHORED BY - SAUMYA GUPTA

Abstract:

With the advent of the digital era, governance in India has undergone a change from a lengthy paper trail to a speedy connection to government, in which an individual can obtain vital papers via digital platforms such as DigiLocker with only a few clicks of the computer with no roadblocks in their way. This article will look at DigiLocker as a digital governance tool and its role in the administrative law perspective to further obtain the answer to a key question: While DigiLocker improves the efficiency and effectiveness of government, does it also compromise privacy and accountability for individuals? On the one hand, DigiLocker has made such an improvement, as it provides an easy way to verify documentation, minimizes the requirement for carrying paper documents, and promotes transparency. Given its ability to provide such improvements to the user's experience with the government, this system falls perfectly within the concept of Digital India as it enhances user experience with government. On the other hand, because the majority of the system is formed through delegated legislation which gives the power to the government to promulgate rules, it is possible for rules to be promulgated in such a way that they are able to provide an opportunity for the government to act without proper accountability. This possibility is present because of the flexibility provided under such delegated legislative authority and may create the potential for greater use of government authority without accountability to Parliament.

Keywords: Digi-Locker, Digital Governance, Delegated Legislation, Government, Parliament.

Statement of Problem:

Digital Governance in India, especially with projects like DigiLocker, has become very popular. This surge has almost doubted about the number of people using government services. The result? Faster responses ad a big drop in the need for physical paperwork to access these

ISSN: 2582-6433

services. However, this evolution demonstrates progress and modernizing the way citizens access their government. It also creates a multitude of administrative/legal challenges that have not been sufficiently tackled to date. DigiLocker sits at the intersection of law and technology; however, the legal framework that governs the operations of DigiLocker—based primarily on delegated legislation—raises issues regarding the legitimacy of executive power and the adequacy of oversight mechanisms. As such, there is a need to understand whether the current regulatory framework is appropriately positioned to yield an equitable balance between administrative efficiency and the constitutional protections afforded to individuals.

The growth of delegate laws regulating digital platforms such as DigiLocker has created a potential problem of too much power being put in the hands of an executive body, making it easy for that body to convene a committee to determine whether to take action. Since these laws do not provide for established procedures to create new rules or to ensure accountability, it will be increasingly challenging for regulators to police themselves.

Another important part of this issue is protecting people's privacy. DigiLocker stores and shares sensitive personal information, like Aadhar Cards, PAN Cards, and other official and personal documents. This kind of information is open to many threats in an electronic environment, such as unauthorized access, data breaches, and other possible misuses. Even though privacy is a basic right, its not clear how well DigiLocker protects users' data. More questions need to be asked about how much control users have over their data, how much responsibility the government has for making sure data is stored safely, and how much control users have over their data. People are more tensed about their data privacy which is about the possible breaches of trust or failure to protect them from unauthorized access as these concerns are not clearly enforced. At the same point of time, the increasing use of digital platforms by users for delivering them their required services to the users raises questions about the accountability of government in decision-making processes.

As technology becomes more involved in decision-making, it may become less clear to the average person about how these decisions are made. This creates a gap between the improved efficiency of services delivered and the accountability of the decision-making process, where the average citizen can get services faster but can't hold the decisionmaker accountable for their actions. The main question this paper is trying to answer is how to balance the efficiency provided by the digital governance tools like DigiLocker with the basic principles of Administrative Law regarding the privacy, transparency and accountability.

ISSN: 2582-6433

Table of Contents:

ISSN: 2582-6433

Introduction:

The shifting of the procedures of administrative process from paper mode to electronic mode, the digital era in the governance has rapidly modified how the State should interact with the citizens. This kind of alternation has been initiated in India as a form of Digital India. This type of project has converted into a technology-driven country which has become more transparent, accessible and effective. DigiLocker is an initiative taken by the Government of India and launched as a flagship programme whose objective is to transform the into a digitally recognized state and technologically advanced country. Digital India is one of the most crucial project. Digiocker has emerged as an important upgradation tool which enables the citizens to access, store, and can share the government related important documents in an electronic form and also in an authorized manner.[1]

The Ministry of Electronics and Information Technology (MeitY) commenced the programme of DigiLocker in 2015. The functions of DigiLocker is a cloud-based storage system electronically where the important government records or documents of the users can be stored in an electronic way and making it authorized as well as safe for the users. The use of this electronic cloud-based storage has reduced the problem of physical documentation and also helps in streamlining verification processes.[2] It is programme through which any person can get real-time access to dematerialize their documents or certificates, Aadhar Card, Driving License, PAN Card, Certificates of High School and Inter School, etc. they can be accessed in DigiLocker which is being issued by various government organizations performing their respective functions through online mode. The objective of launching this programme is the reduction of physical documentation and moving towards in the digital era by utilizing the resources at its best. The documents which are issued here are authorized by respective government bodies and also gives security by the Government organizations.

The documents of the users listed here are legally recognized by the government bodies that is of utmost importance as of the physical documents of the users under the Information Technology Act, 2000. As well as the rules and regulations framed by reinforcing its legality within India's legal framework.[3]

[1] Ministry of Electronic and Information Technology, Digital India Programme (Government of India).
[2] Official Platform overview, DigiLocker, Government of India.
[3] Information Technology Act, 2000; Information Technology (Preservation and Retention of Information by Intermediaries providing digital locker facilities) Rules, 2016, Rules, Rule 9A.

ISSN: 2582-6433

DigiLocker has enhanced the administrative efficiency, but it also has some problems like in legal as well as in constitutional sense. The operational framework of DigiLocker is governed through delegated legislation, to be precise Information Technology Act, 2000 (Preservation and Retention of Information by Intermediaries providing Digital Locker Facilities) Rules, 2016.[4] Delegated legislation allows the government to quickly deal with technical changes, but it often works with little oversight from Parliament, which raises concerns about transparency and democratic accountability.

DigiLocker also raises privacy concerns because of the way it stores and processes all types of private personal data in one single database. The fact that privacy has been recognized as a fundamental human right under Article 21 of the Indian Constitution has led to increased scrutiny of the digital governance systems that involve the collection and distribution of data on such a large scale.[5]

The Digital Personal Data Protection Act, 2023 is an effort made to regulate how the organizations can process the personal information and protect the sovereignty of individuals over their own personal data. Nonetheless, many doubt that this new law will reduce the risks posed to citizens' privacy when their data is collected and held by the government through an open data catalog.

DigiLocker is a major step in India's movement toward a completely digital and paperless government by providing citizens with a safe, efficient way to store, retrieve and share their records. DigiLocker is also vital to the Digital India Initiative because it helps eliminate the usage of paper-based documents in favor of digital documents and creates access to official, digitally issued documents and certificates. The Digital Personal Data Protection Act, 2023 symbolizes a need for regulating the processing of data activities and also to protect the individual anatomy, however, the issue remains there only that is about the checking its adequacy in addressing the State-led ecosystems.[6]

[4] Information Technology (Preservation and Retention of Information by Intermediaries providing digital locker facilities) Rules, 2016.
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[6] Digital Personal Data Protection Act, 2023.

ISSN: 2582-6433

Chapter II: Concept and Legal Framework of DigiLocker

A tremendous advancement in digitalized governance is represented by DigiLocker as this tool allows individuals to securely, conveniently and reliably save, retrieve, or share successful authenticated digital copies of their records via the internet. DigiLocker provides an opportunity to replace physical records with their digital counterparts.[7] This was also a key strategy under Digital India: to create an environment for reducing the reliance on physical documents and moving towards a paperless route of delivering services by the government to its citizens.[8] It functions like a cloud-based storage unit that provides people with a means to save their digitized authoritative proof (certificates, documents etc.) in a manner that facilitates quick retrieval for verification and other purposes.

Chapter 2.1: Concept and Operational Framework:

To create a digital document wallet that contains a user's ID, DigiLocker's primary objective is to use Aadhaar as a common point of identification. DigiLocker database includes three user types: issuer, requestor and users.[9] Issuers include government agencies and others with rights to create and upload documents digitally (e.g., driver's licenses, vehicle registration, school documents). Requestors include the general public and students who wish to check these documents to confirm their authenticity. Requestors of DigiLocker include employers and universities as well as any governmental authority establishing rules or regulations.

One of the major advantages of using DigiLocker as an Issuer is the use of URIs to retrieve documents directly from an Issuer's data storage instead of uploading them. This process provides the assurance that the document is valid and minimizes the likelihood of this document being fabricated. Furthermore, DigiLocker integrates e-signatures and digital signature solutions, making the document legal and tamper-evident. DigiLocker also provides a method for confirming information in near real-time and a simple means of sharing information, thus increasing the efficiency of the transaction significantly.

Chapter 2.2: Legal Framework Governing DigiLocker

The main law that governs the applicability of DigiLocker is the Information Technology Act, 2000. It provides for legal status for electronic data and also of digital signatures. In particular, section 4 of the Act states that electronic records will have the same effect as physical records,

[7] Ministry of Electronics and Information Technology, Digital India Programme (Government of India).
[8] DigiLocker ecosystem structure (issuers, requesters, users).
[9] Integration of e-sign and digital signature under IT Act, 2000.

ISSN: 2582-6433

provided they conform to the requirements of the Act;[10] this provision provides for the use of DigiLocker documents for official transactions.

In addition to the primary legislation, DigiLocker is also subject to secondary legislation, namely, the Information Technology Rules (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities), 2016.[11] These Rules create the framework under which DigiLocker operates, and they set out the expectations of service providers, issuers, and the Digital Locker Authority.

The Rules require that there be a Digital Locker Authority. The Digital Locker Authority is an agency of the central government that ensures the appropriate use and regulation of the DigiLocker ecosystem. The Authority ensures that standards are met and to supervise service providers and develop procedures for the retention and security of data.

The Rules also provide for the equivalency of documents issued electronically and those issued physically for legal purposes. The legal equivalency of electronically issued documents has been reinforced through various amendments and government notifications.

Chapter 2.3 Role of Delegated Legislation

The regulation of DigiLocker through delegated legislation is essential for its effective management. It allows the government to create specific rules and regulations, but only within the framework of the Information Technology Act, 2000. The flexibility of the delegated legislation system allows for adaptability to changes in technology or to suit the needs of the government. This increases concerns about the ability of the executive to make rules and also the limited powers of Parliament in reviewing the executive's decision-making ability.[12]

The rules will mainly govern the operational processes and data management, including access protocols and security standards for DigiLocker. Developing the operational procedures, data management and access protocols will ensure that they are operating in an efficient, smooth manner; however, they also highlight the need for strong monitoring systems in place to prevent the misuse of provisions, and holding people accountable for their use.

Chapter 2.4: Interface with Emerging Data Protection Laws

DigiLocker is governed by digital laws such as Data Protection whose legal requirements have

[10] Information Technology Act, 2000.
[11] Information Technology (Preservation and Retention of Information by Intermediaries providing Digital Locker Facilities), Rules, 2016.
[12] Functions of Digital Authority under the 2016 Rules.

ISSN: 2582-6433

evolved due to recent statutory provisions like the Digital Personal Data Protection Act, 2023[13] which establishes a consent-based paradigm for processing data through fiduciaries (data holders) and reliance on fiduciary duty by Data Holders; Therefore, because DigiLocker maintains sensitive data regarding individuals and non-individual or public trust level rules regarding personal interactions there is a clear need to adhere to Data Theft Prevention Policy and Procedures in order to ensure compliance with federal data protection laws protecting consumers and retaining a level of public trust.

Chapter III: DigiLocker and Administrative Efficiency

The government has been becoming more efficient due to the use of technology, and as an example DigiLocker is the best example to explain it. It has made its services better for public for their usage by using it by digitalization of storage, distributing documents, and checking them. The rule of e-governance is used for making administrative tasks to become easy, and quick.[14]

Chapter 3.1 Lessening of Bureaucratic Steps

DigiLocker helps in reducing the time and effort of people while spending and dealing with their physical documents if all their files were now in electronic format. Before DigiLocker existed, if you needed to provide multiple copies of your documents (usually signed by an authorized individual) for some sort of administrative process, you would have had to send these documents in hard copy, causing delays in completing those processes and overall inefficiencies

With DigiLocker, you can retrieve authenticated electronic versions of your government-issued documentation, removing the former need for the involvement of many individuals and eliminating the possibility of corruption with less reliance on the use of middlemen and manual verification processes.

Public authorities now have the ability to verify documentation instantaneously, allowing for a quicker turnaround in decisions made regarding applications for admission, licensing, job verification, etc.

[13] Digital Personal Data Protection Act, 2023.
[14] Ministry of Electronics and Information Technology, Digital India Programme (Government of India).

ISSN: 2582-6433

Chapter 3.2 Time and Cost Efficiency

DigiLocker can save time and money for both the citizen and the government agency. Eliminating the use of physical paper saves on the costs associated with printing, storage, and transportation of records. For citizens, it saves them time by enabling them to retrieve, carry, and submit documents to various government organizations.

Government agencies can reduce their administrative costs and process applications more efficiently with DigiLocker. By working with different departments using DigiLocker to share information, the need for duplication of work is reduced and therefore increases the overall efficiency of government agencies. Additionally, because documentation can be digitally verified through DigiLocker, it can be verified much more accurately than if it were completed manually with paper-based processes.

Chapter 3.3 Interoperability and Integration

A major benefit of DigiLocker is its operational ability across multiple government platforms and services. Its operation seamlessly integrates with Aadhaar, e-signature services and various department databases to form an all-inclusive digital ecosystem.[15] By doing this, the efficiency of verifying and obtaining documents is considerably improved and ultimately leads to an accelerated delivery timeline for services provided through DigiLocker.

For example, transportation authority's allow citizens to easily verify and obtain their driving licenses and motor vehicle registration certificates through their respective websites (which are connected back to DigiLocker). Similarly, various educational institutions and boards now provide electronic copies of educational certificates and thus there is no longer any need for physical verification.

At the same time, other APIs (Application Programming Interfaces) have also greatly improved the interoperability of systems and therefore the speed at which data is able to flow within and between digital platforms. Without the services and architecture that are explicitly designed to connect all of the digital systems, Digital India would not meet its objectives.

Promotion of Paperless Governance:

A fundamental element associated with digital Governments is digital Documents known as DigiLocker. DigiLocker is intended to increase the usage of non-physical, or "paperless" government as part of a longer-term plan to modernize a number of different aspects of our

[15] Integration with Aadhar and e-sign services under IT Act, 2000.

ISSN: 2582-6433

administrative processes.[16] In so doing, by decreasing our dependency upon paper documents, DigiLocker assists with environmental sustainability by enabling the formation of efficient low carbon models of governance.

Digital documentation allows for the retention and retrieval of documentation digitally, thereby supporting the concept of reducing bureaucracy, and increasing efficiency within the system for providing services to citizens. Having more access to records, documents and processes makes it easier for the public to understand government processes in a clearer manner, thus making voters more informed and governments stronger.

Chapter 3.5 Enhancing Transparency and Trust

The concept of transparency relates to governance. DigiLocker works towards improving transparency by allowing users to utilize a secure and reliable method for managing their documents. Since documents are created only by authorized entities, and can only be retrieved through secure means, there is less risk of forgery.

By creating an environment where users can easily verify the authenticity of documents they obtain from government agencies, a positive relationship can develop between users and their respective government agencies. Transactions completed through DigiLocker also provide a digital history of the transaction, which increases the accountability of individuals doing business with each other while reducing the likelihood of fraudulent activity.

Chapter 3.6 Limitation and Practical Concerns

Chapter 3.6 Limitation and Practical Concerns

There are also potential drawbacks to using DigiLocker that must be addressed if it is going to excel in delivering value. There are serious issues with the digital divide that continue to limit access to those who do not have internet connectivity or digital literacy skills, which could impact their utilization of the service. In addition, technical glitches and server outages can frequently cause service interruptions that affect overall system stability.

The reliance on digital technologies could create a significant vulnerability for the digital systems, especially when faced with both cyber threats and/or system failure. While Digi Locker is designed to improve operational efficiencies, it will be necessary to have the requisite infrastructure and supporting systems in place to support the long-term stability of its operations.

[16] Promotion of paperless governance under Digital India initiative.

ISSN: 2582-6433

Chapter IV Privacy Concerns in DigiLocker

While DigiLocker has enhanced the ability of administrators to perform their duties, there are some significant issues remaining about preserving personal information and privacy of individuals' data. DigiLocker allows for the digitized storage of sensitive personal records, such as identity documents, school transcripts and other financial data. This poses an interesting challenge, due to the intersection of governance and information protection. As fast as our technological dependance is increasing nowadays, there is a need for thorough analysis of the privacy of users who are using Digilocker as their storage for keeping their important documents within India's constitution and other statutory frameworks.

Chapter 4.1 Right to Privacy and Constitutional Framework

In a ruling by the Supreme Court in Justice K.S. Puttswamy v. Union of India,[17] held that the Constitution guarantees all persons the right to privacy as a fundamental right to the right to life and personal liberty, as protected by Article 21 of the Constitution. Furthermore, the analysis and ruling provided that the right to privacy, especially as it relates to the safeguarding of individual's private information, falls within the right to life and personal liberty. This ruling also established that with each and every government activity involving the collection, storage, or processing of an individual's private data, as well as any type (mode) of government collect in order to collect or share an individual's private information are to be established based on the principles of legality, necessity, and proportionality.

Given this backdrop, when considering the context of DigiLocker, the processing performed by the State (and/or by State agencies) and its authorized entities resulting in the storage and/or sharing of someone's personal documents for certain purposes raise serious questions as to whether or not the legal environment regulates the manner in which such collection activity is being carried out in accordance with the standards established in K.S. Puttaswamy (Retd.) v. Union of India.

Chapter 4.2 Data Collection and Centralization

DigiLocker functions using Aadhaar-based authentication to associate each person's identity (via Aadhaar) to many of their different official documentation types.[18] This results in many individuals' personal data being collected and unified into one digital ecosystem. While this centralization makes it easier and more convenient for people to access their personal data, this

[17] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[18] Aadhar-based authentication in DigiLocker ecosystem.

ISSN: 2582-6433

centralization also poses additional risks related to how people use data and how the State can use your data to take action against you. The Centralization of data can allow for extensive profiling and surveillance at the State level.

The State can use all the different data points across diverse application systems (i.e., education, employment, identification, financial status, etc.) to develop an extensive profile of a person. This extends to the area of informational self-determination, a concept that considers how data and personal information can affect individual autonomy.

Chapter 4.3 Risks of Data Breach and Cybersecurity Threats

DigiLocker uses several ways to secure its information on the cloud through Encryption, Multi-Factor Authentication, and Data Centre Security Features; however, this does not mean it is free from Cyber Attacks.[19] If a breach occurs due to unauthorized access to Private Information/Data it can have serious impacts to individuals that have confidential data stored on DigiLocker.

The speed at which Digital Data can be copied or shared means that if a breach occurs that the consequences will be worse than if the data was Paper Based. There is no such thing as Perfect Security Technologies, so Cyber Security Policies must continually be Monitored and Improved.

Chapter 4.4 Consent and Data Sharing Mechanism

Consent is at the heart of DigiLocker which means that users give permission to explore and share their personal documents with other individuals for different reasons. There are many uncertainties with regard to whether or not what is being requested from users is appropriate use of consent if they don't understand all of the reasons why their personal data needs to be necessary, etc., so users may not be familiar with what data has been obtained, how their data was obtained from them and which other names exist.

Informed consent means that in order to give consent for their data, users must be given the ability to specify the exact/complete information as to why their data needs/wants to be shared. Unfortunately, most companies have very little effort to ensure that an individual's privacy is respected.

[19] Security features include encryption and authentication protocols.

ISSN: 2582-6433

Chapter 4.5 Legal Framework: Digital Personal Data Protection Act, 2023

This is a very big step by the government for protecting the data of the users in their protection system. It sets the framework which is depending on the thoughts such as minimizing data, restricting the purpose or use of data, permission. It binds duties on the data protectors for safeguarding the data stored in DigiLocker and also stopping it for any type of unauthorized usage by any person.

It provides the power to the government to control the processing of data and also protecting the rights of users. Some component of this legislation especially those which gives exemptions to the State, have been coitized for weakening the security and privacy protections.[20] Therefore, this legislation provides for controlling the platforms run by government to control them.

Chapter 4.6 Balancing Innovation and Privacy

The DigiLocker system demonstrates the difficulty of reconciling new technology with privacy issues. Although the benefits of having data accessed more quickly and easily outweigh the drawbacks, the larger challenge is that so many people's personal information will be collected and processed as part of this new service. The only way to maintain a balance between these two competing objectives is through strong legal protections, clear governance and enforcement of those laws.

Chapter VII Need for Stronger Safeguards

We can protect privacy by taking three main actions. These actions are:

1. To have stricter rules for how much data can be collected (data minimization)
2. Improve encryption (making your data unreadable to anyone but you) and security for how data is collected and stored
3. Ensure that people know what happens with their personal information (data accountability) and can see how their digital rights are being protected (data transparency).

The above actions will increase DigiLocker's compliance with the Constitution and build trust in the government's digital services.

[20] Criticisms regarding State Exemptions under DPDP Act, 2023.

ISSN: 2582-6433

Conclusion:

The DigiLocker programme has improved the system of digital administration. The main aim of this programme of DigiLocker seeks to improve transparency, accessibility and efficiency for the. It also allows for confirmed electronic data that is to be stored in a safe and secure manner and can shared easily, which enables the faster providing of public services. Thus, reducing delay caused by bureaucracy, lessens dependence on hard-copy documents, and it enhances the overall quality of public service provisions. Furthermore, the legality strengthens under the Information Technology Act of 2000.

Growing reliance on DigiLocker raises serious questions regarding privacy and accountability. When sensitive personally identifiable information is stored in a single database, and when that is supported by the Aadhaar system, there are sufficient justifications for concern over such issues as data privacy, surveillance and potential abuses of stored data. Justice K.S. Puttaswamy v. Union of India established the right to privacy as a fundamental right, thus indicating that any digital infrastructure that relies on this objective should comply with the constitutional standards of legality, necessity, and proportionality.

Democratic Accountability: While delegated legislation provides the regulatory framework with the flexibility and agility required to regulate highly complex technological environments, its operation is generally outside of Parliament's oversight. Thus, there is a risk of excessive executive power, particularly regarding the governance of personal data and the rights of individuals. The issues of transparency and accountability are further complicated by the lack of robust and independent oversight mechanisms.

Although the Digital Personal Data Protection Act (2023) represents an important milestone in the protection of personal privacy, its effectiveness in regulating state-operated digital platforms (e.g. DigiLocker) is still under close observation. An effective regulatory framework will provide a balanced approach so that individuals' rights are not compromised in the name of efficiency.

To summarize, provided that DigiLocker is adapted to the current challenges of digital governance in India and elsewhere, it has the potential to be an exemplar for digital governance. To achieve a balance between efficiency, privacy and accountability, we need to enhance the

ISSN: 2582-6433

protections for personal data, enhance the transparency of delegated legislation and establish independent oversight mechanisms. Only then can DigiLocker realize its principles of accountable and citizen-focused governance.