E-GOVERNANCE AND CONSTITUTIONAL CHALLENGES IN ADMINISTRATIVE LAW: A CRITICAL ANALYSIS

Rahul Shettar, LLM, School of Law Christ (Deemed To Be) University, Bengaluru

ABSTRACT

India e-governance has revolutionized the way the country is offering its services by offering efficiency. Transparency, and engagement of more citizens. And this haste digitalization causes concern. constitutional and administrative issues that require a clear cut analysis. This study paper contrasts the scope of the constitutional provisions of India, (Article 14) (equality), (Article 19) (right to speak) and (Article 21) (right to life and privacy) and the existing administration laws are prepared to handle the legal, ethical and procedural challenges generated as a result of e-governance projects. The effect of the constitutional protection was found to be moderated by the research questions on the sufficiency of the constitutional protection, basic rights is a digital government on the institutional and legal loopholes, data-based problems, and mainstreaming of constitutional protection can be. The research adheres to a dogmatic and analytical research method, digital government. Its objectives are to critically review principles in the constitution that may be applied to e-governance, and to scan the adequacy of administrative law in regulating digital systems, deliberate on effects of digital exclusion to administrative. accountability and rights of citizens, and propose a normative system to encourage constitutional. compliance in e-governance. The analysis of the well-known cases, including the Justice K.S. Puttaswamy vs. Union of India (2017). The paper concludes with Shreya Singhal v Union of India (2015) and the existing academic. literature that constitutional rights are a good starting point, but the administrative. and the legal domain is unprepared to deal with an algorithmic prejudice, data privacy. violation, and internet marginalization. The paper concludes that such incorporation of the constitutional protections This is necessary in e-governance systems to make sure that there is effectiveness in technology in accordance with the basic rights of citizens, transparency, equality and, thus, create a rights-based and inclusive. digital governance system.

Keywords: Constitutional Rights, Digital Governance, Privacy, Data Protection, Algorithmic risks, E-Governance, Administrative effectiveness, Digital divide, Global, National security, and Cybersecurity Concerns.

1. INTRODUCTION

With the advent of digital technologies, the world has changed the methods of government service delivery and the relationship between people and the government. In India, such programs as Digital India,[1] e-Kranti,[2] Aadhaar[3] and DigiLocker and other state-level digital programs can be observed as a result of this transformation. Such programs are designed to make sure that governance becomes more citizens friendly, transparent and effective. E-government can reduce distance between the state and the citizens, reduce corruption, improve service delivery and involve more people in the democracy. Nevertheless, being very timely, it has serious constitutional and administrative problems. Privacy, equality, freedom of expression, accountability and access to justice are the main aspects that determine whether the governance system of India is prepared to the digital age.

The biggest problem is the constitutional protection and efficiency in technology trade off. Digital governance is quick and affordable to the masses, but it can also reveal underlying rights in a situation whereby personal data are misused, in which the expression of surveillance is excessive, and where and when people are marginalized because of digital illiteracy or lack of infrastructure.

The rulings passed in the courts like Justice K.S. Puttaswamy case[4] and The case of Shreya Singhal (2017),[5] which implicated that privacy is one of the fundamental rights proclaimed that union was a fundamental right. The constitutional regulations can be changed according to the new technology as observed in the case of Union of India (2015), which provided protection to the freedom of speech via the internet. However, these principles may not be implemented in practice without the existence of strong laws and administrative institutions. The old Information Technology Act, 2000[6] and the slow pace of creating comprehensive data protection laws reflects the lack of statute in the regulation of contemporary issues of algorithmic bias, cybersecurity threats, and machine learning decision-making. An increasing body of literature focuses on these trends. Other scholars, such as Lekshmi Viswanath,[7] view

[1] Digital India Programme, Ministry of Electronic & Information Technology, Govt of India (2015).
[2] e-Kranti: National e-Governance plan 2.0, Ministry of Electronics & Information Technology, Govt of the India (2014).
[3] Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act, no. 18 of 2016.
[4] *Justice K.S. Puttaswamy (Retd.) v Union of India,* (2017) 10 SCC 1.
[5] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1
[6] Information Technology Act, no. 21 of 2000.
[7] Lekshmi Viswanath, *Digital Constitutionalism: Navigating Governance in the Technological Era*, 2 JOURNAL OF LAW AND LEGAL RESEARCH DEVELOPMENT 1 (2025).

the trends of the "digital constitutionalism," aimed at inscribing constitutional values onto the digital plane. Mohammed Y.[8] and Mamatha U.[9] take the constitutional issues of e-governance in India, citing the issues of surveillance, privacy invasion, and exclusion. The works on this topic by Nagararajan K.[10] and Sugesh S. and Sai Shruthi A.[11] highlight the advantage of initiatives such as Digital India and incorporate such concerns as the digital divide and accountability concerns. In other countries, such authors as Radu[12] suggest that digital technologies are transforming rights and models of governance internationally. However, even the majority of the research studies are policy-focused or theoretical with little empirical examination of the real impact of constitutional rights. In addition, Indian scholarship has not adequately addressed the challenge of how local ground realities, such as rural illiteracy, poor connectivity, poor institutional capacity, are placed in contact with constitutional issues in digital governance. This paper discusses e-governance in India about constitutional and administrative concerns in a very close way. We will see how digital rules will change the basic rights. Organizations and regulations tend to be weak and computer judgments might override old notions of justice and accountability. We would also like to find out how e-governance affects privacy, fairness and justice. The analysis will be done on the failures in the rules and laws in India. We will take into consideration information control risks. We will propose the amendments, which will give constitutional investigation to online regulations. When this is achieved, the research will help the Indians and other individuals in the world to negotiate digital regulations and human rights. It will aim at making sure that the process of converting India to e-governance is not only technically savvy, but also constitutional, open to everyone, and answerable.

2. LITERATURE REVIEW

2.1. Digital Governance and Constitutional Rights.

A relationship between e-governance and the Indian Constitution, namely, Articles 14, 19, and 21 is one of the most popular themes in scholarship. Viswanath argues that although the constitutional guarantees of equality, free speech, and privacy are established, they are ill-

[8] Mohammed Yazeen PS, *Digital Democracy: Constitutional Challenges in the age of E Governance*. 5 INTERNATIONAL JOURNAL OF RESEARCH PUBLICATION AND REVIEWS 3 (2024).
[9] Mamatha. U, *The Challenges of e-Governance in India: A Critical Analysis*, 5 IJRAR 2 (2018).
[10] Nagaraja K. *E-Governance in India: Issues and Challenges*, 7 IOSR JOURNAL OF ECONOMICS AND FINANCE (IOSR-JEF) 5 (2016).
[11] Sugesh S. & Sai Shruthi A., *Models of E-Governance: Constitutional and Administrative Perspectives* (2022).
[12] Giovanni De Gregorio& Roxana Radu, *Digital constitutionalism in the new era of Internet governance,* 30 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY, (2022).

formed in the context of applying to the digital world and legislators and the courts are lagging behind in the provision of substantial protection.[13] Mamatha puts projects of e-governance like Aadhaar and Digital India into the framework of basic rights, which also encourages their potential of transparency but also their potential of disenfranchising citizens who have low digital access.[14] Both studies underscore the idea that digital governance could not be isolated of constitutional guarantees, and insist on the need of a law and legal science that would convert the basic constitutional values into technology facts. This is the point that Malik takes in his argument where he warns that cyber-insecurity, mass surveillance, and data misuse may erode these very rights unless the right measures are enacted to prevent it.[15] All these studies demonstrate that the constitutional foundations of India are strong, but their implementation in the online environment is uneven and requires redefinition and modernization.

2.2. Algorithms, Data Protection, and Privacy.

One of the important constitutional matters of e-governance discussion is privacy. In his study, Mohammed warns that the Aadhaar type and DigiLocker type of platforms as they draw more citizens on board, also harvest sensitive data without proper safeguards, thereby endangering constitutional liberties.[16] Dalal and Richa address this dilemma unilaterally, demonstrating that Digital India and e-Kranti initiatives enhance the delivery of services and strengthen the power of the state to regulate personal data, at the same time.[17] They argue that without a robust data protection, the right of privacy of the citizen is violated. Malik substantiates this by illustrating how leaks, discrimination, and unsecured systems damage the trust of the government and might end up draining the constitutional liberties.[18] These books arrive at the conclusion that the safeguarding of privacy is a constitutional and practical necessity to ensure that citizens have confidence in the government.

2.3. Administrative Effectiveness and E-Governance Models.

There is, however, another significant group of scholarship that talks about models and administrative mechanisms of e-governance. Sugesh and Sai Shruthi present the concepts G2C,

[13] Lekshmi Viswanath, supra note 7
[14] Mamatha. U, supra note 9
[15] Rituraj Malik, *Cybersecurity and National Security: Constitutional Issues in Digital Governance*, 11 IJARIIT, 2 (2025).
[16] Mohammed Yazeen PS, supra note 8
[17] Priyanka Dalal & Richa, *e-governance and privacy: Analyzing the privacy implications of digital government initiatives in India*, 11 RESEARCH HUB INTERNATIONAL MULTIDISCIPLINARY RESEARCH JOURNAL. 10 (2024).
[18] Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act, no. 18 of 2016.

G2G, and G2B with reference to efficiency and corruption control in Aadhaar and Bhoomi projects.[19] They refer to the fact that success is not measured against such principles of the constitution as privacy or equality. Likewise, Nagaraja provides a descriptive overview of Digital India and e-Kranti efforts and glorifies the institutional development without taking a closer look at the constitutional analysis.[20] On their part, Kalsi and Kiran elaborate on the determinants of success of state projects like Bhoomi and Suwidha emphasizing that they require training, inter-departmental coordination, and secure environments.[21] In their publication, they point out the fact that effective administrative systems can help in ensuring that the judiciary is accountable. All these studies have shown that despite the fact that models of e-governance are technologically appealing, there is no constitutional foundation to support them.

2.4. Exclusion, Inclusion, and Digital Divide.

Many of the writers note that e-governance though appealing is a source of exclusion unless it is inclusive. Mamatha acknowledges that digital illiteracy and lack of connectivity excludes marginalized segments, which would be a threat to the violation of equality under Article 14. Another important fact mentioned by Nagaraja is the unwillingness to bridge a digital divide, and mistrust of Internet systems, which are undermining citizen trust. The bottom-up approach is introduced by Madon, who shows, using the examples of Gujarat, Kerala, and Karnataka, that good governance is based not on a universal technological fiat,[22] but on the local social networks and the involvement of the population. She feels there is a break in the literature concerning incorporating the view of the people in models of governance. All of these studies together show that e-governance may reinforce inequality rather than eliminate it in the absence of the focus on exclusion.

2.5. International and Universal Views.

A less, though still significant, group of literature repositions Indian discussions in the international arena. De Gregorio and Radu argue that the current digital technologies in the world are reconstituting the constitutional freedoms and rights politicizing the internet as a constitutional and political space.[23] They highlight in their publication that constitutional

[19] Sugesh S. & Sai Shruthi A, supra note 11
[20] Nagaraja K., *E-Governance in India: Achievements, Challenges, and Constitutional Issues* (2021).
[21] Nirmaljeet Singh Kalsi & Ravi Kiran, *Determinants of Success in State E-Governance Projects: A Constitutional Viewpoint* (2020)
[22] Shirin Madon, *E-Governance in Rural India: A Developmental and Constitutional Perspective* (2023).
[23] Giovanni De Gregorio& Roxana Radu, supra note 12

matters of e-governance are not unique to India but are instead a world-wide transformation in the way governance and the protection of rights is carried out. Their analysis is more abstract, but the comparative ideas presented in it contribute to the Indian scholarship by putting local issues in a world discussion.

2.6. National Security and Cybersecurity Issues.

Insecure systems, surveillance technologies, and discriminatory algorithms are some of the threats to the constitution identified by Malik, who warns that they are against basic freedoms. His belief in encryption, limited data gathering, and responsibility tools highlights the precarious nature of the national security and the constitutional liberty. He is critical in his work in showing that digital insecurity is not merely a technical issue, but in a more fundamental constitutional sense, it affects rights under Article 19 and 21.

Synthesis and Gaps

It is possible to make several observations through these thematic clusters. First, authors unanimously pinpoint the tension that exists between the effectiveness of e-governance and the protection of constitutional rights. Second, the most important constitutional problem is that of privacy, but the citizens are vulnerable due to poor statutory and procedural safeguards. Third, although this research discovers exclusion, digital divides, and administrative scarcity, it hardly links such problems to enforceable constitutional guarantees. Fourth, the Indian scholarship does not exhaust the international experiences in spite of the benefits they may have.

Gaps also stand out. The literature is sparse in terms of empirical evidence on how rights in practice are affected on the ground and thus most of the analysis is doctrinal and theoretical. Solutions-oriented research is also sparse, and even writers who identify risks do not describe enforceable constitutional or legal regimes to bridge the gap between administrative creativity and fundamental rights. Finally, citizen-centered approaches, especially ones that involve the community and locally-based policy-making, have limited research.

According to literature, Indian e-governance is currently at the stage of constitutional law, administrative efficiency, and technological revolution. Although digital sphere promises to make the system of governance efficient and transparent, it also renders privacy, equality, and accountability unsafe and endangered. The absence of strong legal principles and the impossibility to transfer constitutional protections to the online environment remain an issue of concern. Therefore, future studies and policymaking must transcend the descriptive reports

and address the normative models that would incorporate the constitutional rights into the core of the digital governance. It is at that point that e-governance will fulfill its potential of inclusive, accountable and rights-based governance.

3. E-GOVERNANCE ADMINISTRATIVE AND CONSTITUTIONAL READINESS.

The e-governance is one of the most progressive changes that have taken place in the Indian history. Some of these programs include the Digital India program and Aadhaar that will eliminate corruption and give citizens more chances to express themselves by ensuring that services are more fast. The transition to the digital government is, however, associated with some serious constitutional and administrative concerns. The big question is whether these issues can be handled by the current laws and institutions.

The Indian constitution is good in protection. Articles 14, 19 and 21 equal treatment, free speech and privacy protect the digital citizens.[24] These protections have been added to the courts. In the Puttaswamy case, the Supreme Court declared the provision of privacy as a constitutional right, which restricted the cyber rules.[25] As in the case of Shreya Singhal, the court invalidated an unspecified provision of internet laws that protect free speech in the internet.[26] These cases show that the judicial system revises rights in new technology.

Even with these rights, the government is not ready with these rights in the form of the laws and the bodies governing it. The main law of digital affairs is the Information Technology Act of 2000 that is outdated and covers the problems of artificial intelligence and the big-data implementation, which is not the theme of the Act.[27] The Act is not much interested in the rights of the citizens or what the government must do regarding the internet; but more on cybercrime and electronic transactions.

Data protection is not fully covered by law and this compromises the rights of the nation. It is a start with Digital Personal Data Protection Act of 2023, and various researchers and campaigners think that it enables the State to make many exemptions and makes it harder to intervene in abuse.[28] This raises the problem of unregulated surveillance, data profiling and data abuse. The law will not offer maximum protection as there are no effective checks in the

[24] INDIA CONST. arts. 14, 19, 21.
[25] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1
[26] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1
[27] Nagaraja K, supra note 10
[28] Internet Freedom Foundation, *Analysis of the Digital Personal Data Protection Act*, 2023 (2023).

institutions.

The thing is that there is an inadequate implementation. The implementation of the rights is poor, although the courts recognize those. To illustrate, some people are losing their welfare payments on Aadhaar due to the biometric errors or absence of connectivity or due to ignorance.[29] This unequal treatment is an indication that the government machine is yet to follow the constitutional principles fully.

Other countries, such as the European Union, have tried to fill this gap, with legal frameworks like the GDPR, which include the rights as the priority of the government.[30] Such a system, combining constitutional values and normal administrative practice, has not been had in India.

In short, the Indian constitutional rules seem to be excellent in paper, whereas the law and institutions that regulate the government are decades behind. Parliament and institutions remain in the backyard since the courts have been eager to extend the basic rights to the virtual world. Without doing the renovation of the administrative systems to include the constitutional guard, we are likely to use the digital tools to be fast and innovative without considering the rights and accountability.

4. E-GOVERNANCE AND ITS INFLUENCE ON THE BASIC RIGHTS.

Another key area in the management of the Indian people is e-governance in which welfare, justice, and provision of information to the citizens have been revolutionized. Digital India projects, use of Aadhaar to access services and Web-based dispute resolution will all ensure that the things are faster, more transparent and people will be able to attend a larger number of them. Nevertheless, there are other basic rights such as privacy, equality and the right to justice that are also affected by these tools.

The right that Article 21 has received is that of privacy which is the most essential right. Justice K. S. Puttaswamy case The Supreme Court mentioned that privacy is a right to be observed and privacy of information necessary in the contemporary society.[31] Nonetheless, e-governance collects a lot of data such as Aadhaar biometrics that can be used to carry out surveillance and

[29] Reetika Khera, *Aadhaar Failures Have Resulted in Starvation Deaths: Government Cannot Deny It*, THE WIRE (2018).
[30] Giovanni De Gregorio & Roxana Radu, *Digital Constitutionalism in the New Era of Internet Governance*, 16 INT'L J. CONST. L. 1 (2022).
[31] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1

profiling.[32] The government says that these measures are necessary, to welfare and good government, unless such precautions are strictly observed as the measures will be excessive and open to abuse. Article 14, equality is threatened also by digital governance. Though the e-government projects have the benefit of availing equal access to individuals by removing the middlemen and red tape, it can widen the digital gap. The basic welfare schemes are not provided to those that cannot read, those that lack internet access or those that lack good biometric ID.[33] Such discrimination is harmful to the poor, old, or the discriminated, and goes against the goal of the Constitution, which is the actual equality. Right to justice is also impacted. Online complaints systems and digital court systems can help to make delay less of a problem by making it more transparent. Nevertheless, they also make life of individuals not endowed with technology complex.[34] Use the case of remote court hearings, throughout the COVID 19, it continued court cases, yet it was biased towards people who did not have a stable internet connection or technological capability.[35] Such disproportion is not in line with Article 39A that states that there ought to be equal access to justice.

The other problem is that there has been a loss of the protections against due process. Automated and algorithmic decision making reduces the utilisation of human judgement, however, it is not transparent all the time. When individuals are deprived of welfare based on an algorithm error or biometric problem, they do not know how or why to do it.[36] It is a debilitating acquiescence in this lack of protection which dilutes administrative accountability and defeats constitutional assurances of justice.

The problems have led to the online policy of laying rights internationally. In point, the GDPR of EU sets privacy, consent and accountability standards that attach data protection and human rights.[37] A nation like India, as far as it has entrenched these rights in the constitution, lacks a proper regulatory framework on rights that can ensure digital inclusion and meaningful participation.

---

[32] Usha Ramanathan, *A Decade of Biometrics in India: Resistance and Silence*, 50 ECON. & POL. WKLY. 123 (2014).
[33] Reetika Khera, *Impact of Aadhaar in Welfare: Exclusion and Errors*, 52 ECON. & POL. WKLY. 61 (2017).
[34] C. Raj Kumar, *E-Governance and Access to Justice in India: Critical Perspectives*, 3 INDIAN J.L. & TECH. 1 (2007).
[35] Aparna Chandra, et al., *Virtual Courts in India: A Reality Check,* CENTRE FOR CONSTITUTIONAL LAW (2020).
[36] Anupama Kumar & Nikita Sonavane, *Automating Welfare: Aadhaar and Algorithmic Exclusion*, INTERNET DEMOCRACY PROJECT (2019)
[37] European Union, General Data Protection Regulation, Regulation (EU) 2016/679.

In short, Indian e-governance strategies improve and threaten the basic rights. Despite the advantage of increasing the transparency in services and making them faster, they often have the cost of privacy, equality and right to justice. The constitutional model offers a concrete base, though, without a great deal more institutions and people-centre design, the digital governance might highlight the very rights it is supposed to secure.

5. DIGITAL GOVERNANCE LEGAL AND INSTITUTIONAL GAPS.

The growing trend of the digital government in India is due to the Digital India policy and other services that make use of the Aadhaar. Though, it is fair that these technologies are supposed to make the government work faster, more transparent, and involve people, it also shows a serious weakness in the institutions and laws according to which machines make decisions. These loopholes compromise the constitutional safeguard and place less accountability to the government.

The major concern is weak data protection. Even though the Supreme Court stated that privacy is a right that has fundamental rights in the Puttaswamy case,[38] India has yet to develop a strong data-protection law. The new Digital Personal Data Protection Act of 2023 is also considered to be criticized in that it offers many exemptions to the state that will diminish responsiveness in the surveillance and data processing.[39] This exposes them to profiling, abuse of their personal data and requires undercover algorithmic choices.

The second issue is that automated decisions lack transparency and accountability. Black boxes are the algorithms which are employed in making welfare payments, predictive police or public services. Whenever someone is denied a good or something they are attacked they are barely explained with a clean cut explanation.[40] This unfairness violates procedural guarantees and Article 21, and the general principles of a decision-making founded on reason and the natural justice can hardly be used to obscure algorithms.

The third weakness is a bad institutional accountability. The government institutions that are currently in place are not trained and empowered to contain the digital technology. IT regulators or data-protection commissions are often not much independent, and are not well-financed as

[38] *Justice K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1
[39] Internet Freedom Foundation, supra note 28
[40] Danielle Keats Citron & Frank Pasquale*, The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014).

watchdog organisations.[41] In comparison to the GDPR of the European Union, where accountability of algorithms is implemented, in India, there is no decentralization of the executive authority, and little checks and balances in protecting the rights of the citizens.

The other problem is digital exclusion which has been experienced by most disadvantaged groups. The assumption of automated rule-making is that everyone is digitally liberated and connected irrespective of low-quality broadband, biometric breakdown, and lack of device.[42] The fact that Aadhaar authentication cannot provide food rations or pensions is a demonstration of how the system can fail, which undermines equality under Article14 and the duty of the government to be an inclusive institution.

And, the last yet not the least, the judicial system is responsive. Courts have also intervened in this form of case as in Shreya Singhal when the court overturned Section 66A in the interests of protecting online free speech, but lacks a systematic legal theory of algorithmic governance.[43] The issues are solved on a case-by-case basis, and the proportionality and fairness of automated systems are not considered. In short, the Indian digital governance is decentralized and outdated. The loophole in the regulations is created by lax data protection, black box algorithms, lax oversight, digital exclusion, and reactive courts. To respond to this, India must implement a transparent, rights-based regulation that inculcates constitutional values in digital governance. The state of democracy will not contribute to reform on the issue of automated decision-making.

6. DATA-DRIVEN DECISION MAKING AND ALGORITHMS: LEGAL ISSUES.

These trends of greater use of algorithms and data-driven decision-making to the government have offered not only new points of efficiency but also created new legal problems which directly suggest new ideas to the rights of citizens and administrative accountability.

The essence of the problem is the fact that the system of algorithms is not transparent enough and is also known as the black box problem. In this instance, the motivation of a welfare, forecast of the crime or resources distribution is hidden to those who are being ruled by the decisions. This blind move violates the constitutional right to equality (Article 14), the right to

[41] Nirmaljeet Singh Kalsi & Ravi Kiran, *Success Determinants of E-Governance in India: An Administrative Perspective*, 12 J. E-GOVERNANCE STUD. 45 (2022).
[42] Reetika Khera, supra note 29
[43] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1

due process (Article 21) and the right to information.[44]

One of the important legal issues is algorithms bias. The same data is used to teach the algorithms and therefore it is likely to reinforce the social inequalities. By implication, when a welfare system is informed, through the historical economic imbalances, the disadvantaged groups may be demoted to access state benefits.[45] This goes against the equality and non-discrimination promise. These are beginning to fall under the jurisdiction of the courts around the globe; in State v Loomis (Wisconsin, USA). The sentencing predictive algorithm known as Loomis (Wisconsin, USA) was challenged, as the accused did not have any opportunity to challenge the algorithm decisions.[46] Although this is not an Indian case, it illustrates the general problem of fairness and due process in making an auto-decision.

Another serious issue is digital exclusion. The disconnected individuals who are not computer literate, do not have access to internet and have no access to relevant devices are often left in the digital government. This introduces another type of inequality: the right to attain rights and services has become technological. The Aadhaar authentication system has deprived the people who cannot verify the biometrics of welfare according to the scholars, and this has led to extreme problems like death due to starvation.[47] Such kind of exclusion is going against Article 21 of the protection of life and dignity, and therefore administrative responsibility is essential.

More legal risks are also caused by weak data protection regime. In spite of such statements by the Supreme Court of India in Justice K.S. Puttaswamy case[48] privacy has been proclaimed to be a fundamental right. India does not also have a similar law in the GDPR of the EU. On algorithmic systems, there is a risk of misuse of personal information without proper protection that leads to identification, surveillance and discrimination. This waterdowns responsibility and puts the citizens at the risk of invasion of privacy with no proper redresses.

It is also significant that it is transparent and explainable. In the instances of automated administrative decisions, the parties with interests are not able to challenge the mistakes in such instances because they lack the knowledge about the logic of the algorithm, as well as the information applied. According to the views of legal experts, explainable AI in the government is required to have due process since decisions should be understood and be subject to appeal.[49]

[44] INDIA CONST. arts. 14, 21.
[45] Mamatha. U, supra note 9
[46] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[47] Reetika Khera, supra note 29
[48] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1
[49] Giovanni De Gregorio& Roxana Radu, supra note 12

Without this, the citizens would be left without redress and the government agencies would not be accountable.

Overall, the idea of data-driven governance and algorithmic decision-making is related to serious legal concerns. They undermine constitutional protections of equality, privacy and due process, amplify digital exclusion, and undermine transparency. To keep administrative accountable, India would require to add more legal enforcement of the algorithms or reform the existing systems to introduce transparency in algorithms, law on data protection and other mechanisms that ensure that the vulnerable citizens do not get disqualified by the digital means. Otherwise, e-governance will merely turn into a constitutional liability and not an administrative asset.

7. INCORPORATING CONSTITUTIONAL PROTECTION IN E-GOVERNANCE.

The new opportunities of more efficient, open and people-oriented services are presented by the changing Indian government digitalization. Nevertheless, it also implies such risks as the loss of privacy, discrimination of some users, and biases. To make e-governance an empowerment, not a dilution, of our constitution, we must incorporate constitutional guarantees in it. This will require ideas and principles that would balance the advances in technology with the right to equality, freedom and dignity.

The reason is that the constitution has its way. Article 14, 19 and 21 must guide every section of the digital government including the manner in which data are gathered and provision of services. Article 14 does not presuppose any kind of discrimination and fairness, and hence the algorithms and platforms must not be developed in a bias manner and must serve the needs of all the people.[50] Article 19 provides the right to know and say, and therefore e-governance ought to offer open access to the decisions making process and ought not to filter any content without justifiable reasons.[51] Article 21 is concerned with privacy and respect and it is the duty of the state to protect personal information and prevent espionage.[52]

These ideas should be maintained by implementing them in institutions. The data protection legislation must be a strong free-standing legislation. Digital Personal Data Protection Act of 2023 is a move in the right direction, yet states have several exceptions that can make the

[50] *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3
[51] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1
[52] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1

mentioned safety measures pointless.[53] A more elaborate framework would require surveillance and data gathering to be done when necessary and that access should be accessed by the courts and algorithms used in law and welfare be audited and affected.[54]

The second pillar is that we must also be just in running of things. E-government sites must also be equipped with simple ways through which one can complain in any language and simple to understand so that a person who could not get what he/she was meant to get due to glitches can receive help.[55] The law also should force agencies to give information on the nature of automation, and the good examples are GDPR to the EU where people are entitled to seek clarifications.[56]

Third, constitutive based protection should be inclusive. The existence of a real digital government that fails to note the digital gap is impossible. Certain policies must provide the cheap internet service, education within the community and offline access to the delivery of vital services. This goes hand in hand with the idea of true equality and it makes sure that the weakest are not left behind.[57]

And finally, the action of courts and parliaments must form a rule-of-law culture. In different situations like Shreya Singhal v. Union of India, has stopped overbearing digital regulations. The court should also review algorithms and tech policy in the future in order to offer compliance with constitutional rules.[58]

In brief, the introduction of the constitutional protection in the Indian e-governance of the nation is not only a coincidence of legislations. It must have a comprehensive system that is founded on equality, privacy, due process, and accountability. Having this kind of protection at the heart of technology, law and culture, India can be in a position to establish a new precedent of digital governance, which does not undermine our constitutional values and does not deny us good public services.

8. FINDINGS AND SUGGESTIONS

Findings

Although the constitutional rights have been put in place, they are not entirely guaranteed on

[53] The Digital Personal Data Protection Act, No. 22 of 2023.
[54] Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016).
[55] C. Raj Kumar, supra note 34
[56] European Union, General Data Protection Regulation, Regulation (EU) 2016/679.
[57] Reetika Khera, supra note 33
[58] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1

the internet.

The Constitution of India ensures equality, freedom of speech, and privacy, but in the real world, a number of online platforms abuse these rights.[59] Although, the Supreme Court acknowledged that privacy is one of the essential rights in the Puttaswamy case, these rights are not enjoyed in the day-to-day e-governance.[60]

Our legislation is archaic and it does not fit the modern technology.

The IT Act, 2000, was developed at the time when the internet was still new.[61] It is not about the problems of our time algorithms, artificial intelligence, and big data in government decisions.

The protection of data is loose and the government is too powerful.

The Digital Personal Data Protection Act, 2023 still allows the government to collect and utilize the data of citizens with minimal limitations.[62] This creates the possibilities of abuse, monitoring, and profiling. No algorithmic fairness and transparency rules. The algorithms are applied by government systems in determining the welfare benefits and other services, but no form of legislation has been enforced by any of the governments to compel them to clarify on their decision.[63] Based on this, individuals find it difficult to appeal against bad decisions hence the process is not just. The consequence of digital divide is exclusion. A large number of citizens are not digital with rural, poor, elderly, and uneducated populations being the most susceptible. In this way, they are deprived of online services, which results in inequality. Absence of effective and independent watchdogs.[64] There are no completely autonomous regulatory agencies that oversee misuse of data and the operation of digital administrative systems in the country. The new Data Protection Board is not quite independent.[65]

Suggestions

Enhance the data security, making it stronger and more standalone. This implies that the government ought to cut its exemptions to the Data Protection Act and come up with an

[59] INDIA CONST. arts. 14, 19, 21.
[60] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.
[61] Information Technology Act, No. 21 of 2000.
[62] Digital Personal Data Protection Act, no. 22 of 2023.
[63] Danielle Keats Citron & Frank Pasquale, *The Scored Society,* 89 WASH. L. REV. 1 (2014)
[64] Reetika Khera, *Aadhaar and Exclusion Issues,* 52 ECON & POL. WKLY. 61 (2017).
[65] Internet Freedom Foundation, DPDP Act Analysis (2023).

independent body with the capability of enforcing the adequate utilization of data.[66] Develop explicit laws of algorithmic fairness. What India needs essentially is legislation that will compel the government to open the books of its algorithms and thus hold them accountable. The agencies ought to demonstrate the method of decision making and correct the mistakes within a short period of time.[67]

Enhance equity, create a grievance system that is easy to adhere to. The online platforms must allow the citizens to complain easily, support them in the native languages, and also include the option to seek human interpretation in case of errors in the automated systems.[68]

Close the digital divide. It must be affordable internet, improved infrastructure to transport and sustain the internet, and electronic education, and availability of offline facilities such that no one will be left behind.[69]

Enhance checks by courts and parliament. The parliamentary committees and the courts should actively consider the digital laws and ensure that they do not in any way infringe on privacy rights, equality, freedom of speech.[70] Integrate constitutional principles in all digital systems. In any e-governance project, equality, privacy, and due process are absolute principles that cannot be compromised at all. These rights should guide the creation and application of digital systems.[71]

9. CONCLUSION

e-governance is a new phenomenon to the Indian government. It will streamline work and make it more transparent and empower the citizens. But there are, as we have discovered, there are also serious legal and constitutional problems that come about due to its rapid growth.

In the Indian Constitution, especially Article 14, 19 and 21, equal treatment, freedom of speech and privacy are ensured even in the digital setting. These rights have been applied by the judges to the use of the internet through the case of Justice K.S. Puttaswamy vs Union of India and Shreya vs Union of India. Our research is behind in terms of government laws and bodies. The IT Act of 2000 is obsolete and the Digital Personal Data Protection Act of 2023, despite being more efficient, still, allows plenty of special state regulations.

---

[66] Id.
[67] European Union, General Data Protection Regulation, Regulation (EU)2016/679.
[68] C. Raj Kumar, *Access to Justice and E-Governance,* 3 INDIAN J.L. & TECH 1 (2007).
[69] Shirin Madon, *E-Governance and Development*, 36 INFO. TECH & PEOPLE 112 (2021).
[70] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1.
[71] *E.P. Royappa v. State of Tamil Nadu,* (1974) 4 SCC 3.

These issues as algorithm prejudice, digital exclusion, and ambiguity are not resolved fully. This destroys accountability and trust. The study shows that e-governance can bring increased accessibility of services but it is also a threat to privacy, equality and justice unless it is well managed.

To wipe this gap, there is a necessity to adopt the constitutional protection into e-government through augmenting data protection, algorithmic accountability, assimilative access, and visible decision-making. The way out however is to continue forward in a moderation between technology and constitutionalism to be sure that e-governance is efficient, democratic, and safeguards the rights of the citizens as well as make inclusive development a reality.

BIBLIOGRAPHY

(ACTS, BOOKS, ARTICLES, REPORTS)

I. CONSTITUTIONAL & STATUTORY MATERIALS

The Constitution of India, 1950

Information Technology Act, No. 21 of 2000.

Digital Personal Data Protection Act, No. 22 of 2023.

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016.

II. CASE LAW

Indian Cases

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1

Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1

E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.

Foreign Case

State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

III. BOOKS

SHANTANU MADON, *E-GOVERNANCE FOR DEVELOPMENT: A FOCUS ON RURAL INDIA* (Oxford Univ. Press 2009).

IV. JOURNAL ARTICLES

Lekshmi Viswanath, *Digital Constitutionalism: Navigating Governance in the Technological Era*, 2 JOURNAL OF LAW AND LEGAL RESEARCH DEVELOPMENT 1 (2025).

Mohammed Yazeen PS, *Digital Democracy: Constitutional Challenges in the age of E Governance*. 5 INTERNATIONAL JOURNAL OF RESEARCH PUBLICATION AND REVIEWS 3 (2024).

Mamatha. U, *The Challenges of e-Governance in India: A Critical Analysis*, 5 IJRAR 2 (2018).

Nagaraja K. *E-Governance in India: Issues and Challenges*, 7 IOSR JOURNAL OF ECONOMICS AND FINANCE (IOSR-JEF) 5 (2016).

Sugesh S. & Sai Shruthi A., *Models of E-Governance: Constitutional and Administrative Perspectives* (2022).

Giovanni De Gregorio& Roxana Radu, *Digital constitutionalism in the new era of Internet governance,* 30 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY, (2022).

Rituraj Malik, *Cybersecurity and National Security: Constitutional Issues in Digital Governance*, 11 IJARIIT, 2 (2025).

Priyanka Dalal & Richa, *e-governance and privacy: Analyzing the privacy implications of digital government initiatives in India*, 11 RESEARCH HUB INTERNATIONAL MULTIDISCIPLINARY RESEARCH JOURNAL. 10 (2024).

Nagaraja K., *E-Governance in India: Achievements, Challenges, and Constitutional Issues* (2021).

Nirmaljeet Singh Kalsi & Ravi Kiran, *Determinants of Success in State E-Governance Projects: A Constitutional Viewpoint* (2020)

Shirin Madon, *E-Governance in Rural India: A Developmental and Constitutional Perspective* (2023).

Reetika Khera, *Aadhaar Failures Have Resulted in Starvation Deaths: Government Cannot Deny It*, THE WIRE (2018).

Giovanni De Gregorio & Roxana Radu, *Digital Constitutionalism in the New Era of Internet Governance*, 16 INT'L J. CONST. L. 1 (2022).

Usha Ramanathan, *A Decade of Biometrics in India: Resistance and Silence*, 50 ECON. & POL. WKLY. 123 (2014).

Reetika Khera, *Impact of Aadhaar in Welfare: Exclusion and Errors*, 52 ECON. & POL. WKLY. 61 (2017).

C. Raj Kumar, *E-Governance and Access to Justice in India: Critical Perspectives*, 3 INDIAN J.L. & TECH. 1 (2007).

Aparna Chandra, et al., *Virtual Courts in India: A Reality Check,* CENTRE FOR CONSTITUTIONAL LAW (2020).

Anupama Kumar & Nikita Sonavane, *Automating Welfare: Aadhaar and Algorithmic*

Exclusion, INTERNET DEMOCRACY PROJECT (2019)

Danielle Keats Citron & Frank Pasquale*, The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014).

Nirmaljeet Singh Kalsi & Ravi Kiran, *Success Determinants of E-Governance in India: An Administrative Perspective*, 12 J. E-GOVERNANCE STUD. 45 (2022).

Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016).

Danielle Keats Citron & Frank Pasquale, *The Scored Society,* 89 Wash. L. Rev. 1 (2014)

Reetika Khera, *Aadhaar and Exclusion Issues,* 52 ECON & POL. WKLY. 61 (2017).

C. Raj Kumar, *Access to Justice and E-Governance,* 3 INDIAN J.L. & TECH 1 (2007).

Shirin Madon, *E-Governance and Development*, 36 INFO. TECH & PEOPLE 112 (2021).

V. GOVERNMENT REPORTS & POLICY DOCUMENTS

Ministry of Electronics & Information Technology, Gov't of India, *Digital India Programme* (2015).

Ministry of Electronics & Information Technology, Gov't of India, *e-Kranti: National e-Governance Plan* (2015).

Law Commission of India, *Reports on Technology and Governance* (various years).

VI. INTERNATIONAL & COMPARATIVE MATERIALS

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119).

United Nations General Assembly, *The Right to Privacy in the Digital Age*, G.A. Res. 68/167 (Dec. 18, 2013).

Council of Europe, *Human Rights in the Digital Age* (2019).