INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

SECURING THE FUTURE: PRIVACY AND PROTECTION IN E-GOVERNANCE

AUTHORED BY - POOJA S P

Abstract

The rise of e-governance has brought significant advancements in the delivery of public services, improving accessibility, transparency, and efficiency. However, as governments increasingly rely on digital platforms to manage services such as identity verification, taxation, and healthcare, concerns about the privacy of citizens' personal data have become more pressing. The digitalization of governance introduces new challenges to safeguarding privacy, raising fundamental questions about data security, surveillance, and the ethical use of personal information. E-governance systems, which aggregate large volumes of personal data for streamlined service delivery, create vulnerabilities that can be exploited if privacy protections are weak or insufficient. Systems like India's Aadhaar or similar digital identity programs worldwide demonstrate the potential benefits of e-governance but also reveal the risks associated with mass data collection, including data breaches and unauthorized surveillance. This has underscored the need for comprehensive data protection laws and privacy-centric frameworks to ensure citizens' rights are not compromised. This paper calls for the establishment of robust legal frameworks and the adoption of privacy-by-design principles in e-governance systems. Leveraging emerging technologies like encryption and blockchain can enhance data security. In conclusion, securing privacy in e-governance is crucial to fostering public trust, ensuring the protection of individual rights, and securing a future where digital governance and privacy coexist harmoniously.

Keywords: E-Governance, Data Privacy, Digital Identity, Cybersecurity, Data Protection Laws

ISSN: 2582-6433

INTRODUCTION

The "e" in E-Governance stands for 'electronic'. Thus, e-governance is basically associated with carrying out the functions and achieving the results of governance through the use of Information and Communications Technology (ICT). The basic objective of implementing e-governance is to enhance governance processes and outcomes with a view to improve the delivery of public services to citizens. At first, e-governance activity initiates through the delivery of information services by government agencies to the public through state websites. The website provides all the information relating to the concerned department, which includes the departmental goals and objectives, its organisational structure, public services and facilities, fees, etc. Thus, in the digital environment, e-governance has emerged as a significant game-changer in relation to how governments interact with citizens. With India now rapidly digitizing, e-governance measures have become increasingly important for it to ensure efficient service delivery, transparency, and accessibility. [1]Now, however, with surging volumes of data generated and processed in e-governance, concerns about the privacy of data have also grown.

EVOLUTION OF E-GOVERNANCE IN INDIA

India's journey into e-governance started in 1987 with the launch of NICENET, a national satellite-based computer network. This effort aimed to connect various departments and improve communication. It then provided a basis for the digital projects that were to be rolled out in the following years, making government services accessible to citizens. The National E-Governance Plan was initiated in 2006 to improve the efficiency and transparency of government services. [2]The scheme consisted of 31 mission mode projects in different areas like health, education, and land records. It aimed at making services accessible and affordable to all citizens so that no citizen is left behind. Later the Digital India Mission was launched in 2015, and it aimed to transform India into a digitally empowered society. This initiative focuses on creating robust digital infrastructure, promoting digital literacy, and delivering government services electronically. The mission has improved the quality of life for most citizens as it makes services more efficient and accessible. Therefore, the evolution of e-governance in India highlights a very significant shift toward using technology for better governance. These initiatives have paved the way for a more connected and informed citizenry, hence enhancing

[1] *National E-Governance Plan* (2006), available at: https://www.india.gov.in/e-governance (last visited Dec. 26, 2024)
[2] National Informatics Centre, *NICNET: A National Satellite-based Network*, available at: https://www.nic.in/history-of-nicnet (last visited Dec. 26, 2024).

ISSN: 2582-6433

the relationship between the government and its people.

KEY E-GOVERNANCE INITIATIVES

India has been taking several innovative e-governance initiatives to make access easier and less complicated for citizens to receive services from the government.[3] DigiLocker is an electronic storage service that enables people to store documents like degree certificates and PAN cards in a digital manner. Therefore, reliance on paper will be reduced, and sharing of documents would be easy. Another prominent initiative is UMANG (Unified Mobile Application for New-age Governance). It is an all-in-one app consolidating access to more than 1,000 government services. It provides access to Aadhaar and PAN-related services. This service is very convenient as it unifies different needs under one interface. Mobile Seva focuses on the delivery of government services through mobile devices. Its applications are over 200 and tailored for direct access through the smartphone. This initiative has greatly improved accessibility, especially for citizens in remote areas, as government services are now accessible to all. These programs collectively represent a giant leap towards digital inclusivity and efficient governance. Initiatives under e-governance in the form of DigiLocker and UMANG change the way citizens interact with the government. Services are available and accessible to citizens at a much higher level through such initiatives.[4] Initiatives like DBT have increased the ease of receiving subsidy and benefits directly into one's bank account. As a result, leakages have been minimized, and welfare schemes have reached those who are in need. This has made it possible for citizens to access a variety of government services online, thus reducing the need for in-person visits to government offices. The programs have also made service access more efficient and easier. During the COVID-19 pandemic, this change has been particularly beneficial as it has allowed people to preserve social distance.

STATE-LEVEL E-GOVERNANCE PROJECTS

Initiatives for e-governance at the state level have drastically changed the way governments provide services to the public, making them more effective, transparent, and accessible. The FRIENDS project in Kerala streamlines the procedure for citizens by providing a single point of contact for paying taxes and other obligations to the state government. The Lokvani Project

[3] Saxena, A., "E-Governance and Public Service Delivery in India: Challenges and Opportunities," *International Journal of Electronic Governance*, Vol. 13, No. 4 (2021), pp. 245–260.
[4] Department of Land Resources, *Digital India Land Records Modernization Programme*, available at: https://dolr.gov.in (last visited Dec. 26, 2024).

ISSN: 2582-6433

in Uttar Pradesh provides a one-stop shop for vital services, land record maintenance, and grievance redressal, guaranteeing accessibility and transparency. By offering an online platform for utility bill payments, certificate issuing, and licence and permit applications, Andhra Pradesh's E-Seva initiative also cuts down on the time and effort needed to access government services. Karnataka's Khajane Project has digitalized the state's treasury system, enhancing the efficiency and accuracy of financial transactions. These initiatives highlight the transformative role of digital governance in improving service delivery and fostering a more inclusive and citizen-centric approach to administration.

BENEFITS OF E-GOVERNANCE

E-governance has many benefits facilitating interaction between governments and the citizens. The first one is that services are accessible 24/7; citizens can visit government facilities any time of their convenience as there are no time-bound constraints. It also saves travel time and money; most services can be accessed online, saving citizens the hassle of visiting government offices in person. It has further ensured that applications were dealt with in a faster mode, thereby reducing delay in an efficient administrative process. Importantly, it promotes transparency and accountability in that it allows citizens tracing the status of their request and promotes openness in the working of the government. So e-governance has been able to improve transparency in government processes and citizens have been able to track status of their applications and payments, which helps reduce corruption and inefficiencies. The improved awareness created by this process evokes greater trust between the administration and its people. Simply stated, this e-governance system transformed the citizen-government nexus with transparency, approachability, and accountability.[5]

CHALLENGES IN IMPLEMENTING E-GOVERNANCE

While e-governance has many benefits, it also has several issues that need to be addressed so that it can be properly implemented. Major issues are that most citizens, especially rural ones, do not have access to the internet and digital devices due to a poor livelihood. Economic inequality continues to limit the services of some groups through e-governance, thus widening the digital divide. Another critical challenge is privacy and security. The increasing concern among citizens regarding the safety of their personal information that is online also raises

[5] Singh, N., "Digital India: Vision, Challenges, and Impact," *Indian Journal of Public Administration*, Vol. 65, No. 2 (2019), pp. 283–293.

ISSN: 2582-6433

issues. Aadhaar and other digital platforms collect massive data which can be misused or there can be breaches of this data which can threaten a citizen's privacy. Then cyberattacks pose risks to sensitive information in the field of financial, health data etc. Sometimes, the unwillingness of government officials and citizens to adopt new technologies is also a problem in progressing. Inadequate training and awareness programs further increase these challenges, making most people unprepared to harness the full potential of e-governance. These are the areas that need to be dealt with to make digital governance inclusive and effective. The success of e-governance relies on overcoming these challenges and ensuring that all citizens can derive benefits from digital services.

One of the main challenge regarding e-governance is privacy issue. Greatest example for this is exploitation of Aadhaar data.[6] In India, an individual's unique identity is registered on the Aadhaar card, and it is mandatory. Through the digital India e-hospital initiative under the ministry of electronics and information technology, an IIT Kharagpur graduate was able to gain entry into the central identities data repository of the Unique Identification Development Authority of India's aadhaar project while the latter was hacking. The software called 'ekyc' transmitted demographic data like name, address, phone number of individuals from the central IDs data depository of aadhaar to authenticate unique identification numbers. It was released on the Google Play Store with the disclaimer that it was framed by mygov, a company connected to the start-up qarth Technologies, after which all the details were made public. Details of an e-hospital system that makes use of Aadhaar to authenticate Aadhaar numbers for his "ekyc verification" app were created as part of the Indian government's Digital India project. This system provides access to all central identity data which is held in the UIDAI repository. A highly qualified technical specialist from IIT, he had a lot of interest in stealing the information from the registered data.[7] This step caused many problems in India, and everyone was worried that when they connected to e-governance, their personal information would have been compromised. likewise Sprinklr controversy in kerala can also be taken into account when we deals with data privacy in heath sector.

[6] Unique Identification Authority of India, *About Aadhaar*, available at: https://uidai.gov.in (last visited Dec. 26, 2024).
[7] Sinha, S., "Role of Aadhaar in Enhancing Service Delivery," *Economic and Political Weekly*, Vol. 53, No. 47 (2018), pp. 38–45.

ISSN: 2582-6433

CAUSES OF PRIVACY RISKS IN ELECTRONIC GOVERNANCE

Despite the careful planning by the government and experts for e-governance projects, privacy issues in e-governance still prevail for a variety of reasons.

Firstly, data privacy would entail securing that data through appropriate gathering and the archiving of personal data. The method of how the data is gathered has also been very crucial to the project. Most information gathered from citizens for this e-governance will be transferred from the already existing records, while more important and recent information will have been directly gathered from citizens.[8]

Therefore, this way of information gathering would turn out to be insecure in case the person who gathered the information misuses the information. Lack of knowledge is the second kind of privacy problem that the vast majority of emerging countries should handle. People not wishing to reveal their information opt to seek outside private companies where help is offered, and once leaks take place in that private organizations, the problem is created.[9]

India has been actively developing its legal framework to address privacy and data protection concerns in e-governance. As public services are getting rapidly digitized, securing citizen data and privacy becomes the priority. The key legal frameworks and initiatives in this domain are:

CONSTITUTIONAL PROVISION

The right to privacy is a fundamental human right recognized globally and has been enshrined in Article 21 of the Indian Constitution as interpreted by the Supreme Court in the landmark case of *Justice K.S.Puttaswamy (Retd.) v. Union of India*[10]. This judgment laid the foundation for ensuring data protection in e-governance initiatives.

STATUTORY FRAMEWORKS

The Information Technology Act,2000 talks about section 43 A which Mandates compensation for failure to protect sensitive personal data by entities handling such data.Section 72 A Penalizes unauthorized disclosure of personal information by intermediaries or service

[8] Department of Land Resources, *Digital India Land Records Modernization Programme*, available at: https://dolr.gov.in (last visited Dec. 26, 2024).
[9] Ministry of Electronics and Information Technology, *Digital India Programme* (2015), available at: https://www.digitalindia.gov.in (last visited Dec. 26, 2024).
[10] **Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1, AIR 2018 SC 4161.**

ISSN: 2582-6433

providers. CERT-In is designated under the Act to address cybersecurity threats and enforce data security measures.

The Digital Personal Data Protection Act, 2023(DPDP Act) was enacted to safeguard personal data in digital form. Key provisions of the act are Data can only be used for the purposes stated during collection, consent based data processing is mentioned, Data protection Board is established to oversee compliance and address grievances. Then entities managing large volumes of data are subject to stricter obligations. But exemption is there broad exemptions for government agencies, raising concerns about potential misuse is also mentioned in the act.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 contains Aadhaar-Specific Regulations. It governs the use of Aadhaar numbers for authentication in e-governance. It also introduced restrictions on sharing Aadhaar data, including biometric information. Then e-governance standards by MeitY (The Ministry of Electronics and Information Technology) is there. It includes Encryption standards for sensitive data,Role-based access control in digital services and Cybersecurity policies for government IT infrastructure.

JUDICIAL INTERVENTIONS

Aadhaar judgment required that Aadhaar authentication should not violate individual privacy. It Prohibited private parties to make Aadhaar mandatory for services. Then in Internet Freedom Foundation Cases Advocacy groups have filed petitions challenging government surveillance projects like Aadhaar, NATGRID, and facial recognition systems.[11]

GLOBAL CONCEPT OF PRIVACY AND PROTECTION IN E-GOVERNANCE.

E-governance has spread all over the world as countries embrace the use of digital platforms for better service delivery and public administration. Among the examples include:
Estonia led the way with its e-Residency, opening its services to worldwide citizens through e-governance. Singapore initiated the Smart Nation project, integrating AI, IoT, and analytics into governance. United Kingdom came up with Gov.uk, a single portal of public services.

[11] *Advocating for Digital Rights: Surveillance and Privacy*, available at: https://internetfreedom.in (last visited Dec. 26, 2024).

ISSN: 2582-6433

International Alignment India follows global levels of privacy standards, which can be seen in India's General Data Protection Regulation to some extent, so much so that it shaped the DPDP Act, and other policies.

RECOMMENDATIONS

It would be possible to deal with privacy and security challenges in e-governance through a more comprehensive legal, technological, and organizational approach. Stiffer laws may provide the impetus needed for effective control over misuse by having stiff penalties for data breaches and violators of privacy. This could be supplemented with extensive public awareness campaigns, whereby citizens are made aware of their rights to privacy as well as the procedures in place for dealing with grievances. All e-governance platforms will integrate privacy-by-design principles, ensuring that security is a core consideration from the outset. Advanced technologies like cryptography can be used to protect data so that it is accessible only to intended recipients. Effective tools for vulnerability analysis must be deployed to monitor and address weaknesses in frequently used applications. Collaboration with organizations like CERT-In is crucial for real-time monitoring and management of cybersecurity incidents, while regular vulnerability assessments and penetration testing are imperative to identify and mitigate potential threats.Promoting multi-factor authentication provides layers of security to a system. Effective grievance redressal mechanisms help citizens bring forth complaints regarding violations of privacy and receive prompt resolutions. In the e-governance platform, anomaly detection can be explored using emerging technologies like AI and machine learning, while encryption and blockchain add layers to data security. These in combination make the framework very resilient in terms of protection of privacy and boosting the confidence of citizens with e-governance systems.

CONCLUSION

In this technological world, privacy is the most precious and also the most vulnerable human right. With new technology, privacy invasion potential has increased and, simultaneously, given more tools to eavesdroppers. Although the digital revolution in governance is bringing us closer to the ideal of good governance, it cannot be termed as an effective and efficient mechanism unless privacy and security concerns are given top priority. The data privacy of a person would be at stake at every stage unless the balance between issues linked to electronic governance and data privacy is resolved with friendly statutory legislation. E-governance is a

ISSN: 2582-6433

revolutionary instrument for improving governmental operations and customer service. It can be used to create not only affordable community facilities but also as a reform tool and a way of changing the government. In this regard, it is highly important to intellectualise, rather than just compete and try to emulate the practical competence of another domain. A safe digital future will be achieved by using the latest technologies, such as encryption and AI-driven security, as well as institutional oversight, and educating citizens on their digital rights. Cooperation between the public and private sectors as well as civic society will be necessary in navigating the complicated terrain of privacy and governance. Hard to envision a success story when a nation-state cannot classify and select a clear, unbiased approach for implementing and utilising electronic governance.