



ELECTRONIC GOVERNANCE AND DATA PRIVACY: A CRITICAL ANALYSIS

INSHAH YASIN¹

¹ Research Scholar, Department of Law, University of Kashmir, Srinagar, India

ABSTRACT

We are living in the age of innovative technological world which has tremendously changed the lives of people and their inter-relation with the government. From the last few decades, the world has witnessed unprecedented growth and dispersal of Information and Communication Technologies in government functioning both in developed and developing countries. It has become a high leveraged enabling tool which has the potential to change the whole process of governance into a new form which relies on Simple, Moral, Accountable, Responsible and Transparent form of governance. It provides wider opportunities for people and business to involve themselves in the process of governance at all levels. The advanced use and application of Information and Communication Technology (ICT) in the government processes has combusted a new revolution which has transformed the conventional relation of Government to Citizen, Government to Government, and Government to Businesses into electronic mode. This new age governance has no doubt paved the way towards achieving the goal of good governance, but at the same time it has resulted in many issues and concerns which acts as a stumbling block in its effective implementation. One of the alarming concerns under e-governance regime is regarding data privacy and security related matters. With every passing time new digital initiatives/schemes and mobile applications are being launched with the purpose of enhancing good governance, but this radical move demands at the same time effective data protection laws with the keen object to protect the ongoing flow of personal data against misuse. This paper attempts to highlight the need and significance of data privacy laws in the present technological driven world.

KEYWORDS Electronic Governance, Information Communication and Technology (ICT), Privacy, Informational privacy, Fundamental right.

INTRODUCTION

Over a decade, the dramatic advances made in the Information Communication and Technology has transformed much of the world in the digital interconnected community. Throughout this period the predominant drivers of change have been the internet and World Wide Web. Both have added a new and indispensable “e” dimension to academia, commerce, and now government. Developments in the information and communication technology have been taking place at a rapid pace. Electronic Governance has been the buzzword throughout the globe in recent times and it’s considered as a worthwhile initiative especially for the developing countries aspiring to make government services accountable, transparent, cost effective, and easy accessible. The involvement of people in ICT enabled governance is significantly different in comparison with traditional form of governance. Digital governance model bring transformation in the existing form of governance as it has changed the citizen government relationship.

¹ Research Scholar, Department of Law, University of Kashmir, Srinagar, India

It may however be noted that there are many constraints and challenges in this momentum of transformation. The significant issues that have become highly relevant for large scale implementation of ICT in governance are the issues of security and privacy concerns. In electronic governance regime, People are left with no other option except to disclose their sensitive personal information for availing government services. In a developing country where people's awareness about privacy is poor and where no comprehensive data protection mechanism is in place, in such paraphernalia the informational privacy becomes the most affected and vulnerable right. Data protection principles are designed to protect the personal information of individuals by restricting how such information can be collected, used, and disclosed. As a legal right, it has developed in many jurisdictions because of the emergence of a wide range of issues related to personal information being processed through automated means. The need for data protection thus arises out of the need to prevent such harms, and hinges on the question of who should be permitted to use personal information and how. The protection of personal information lies at the heart of the right to privacy; and, for this reason, it is an imperative legislative and policy concern.

CONCEPT OF ELECTRONIC GOVERNANCE

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 utilization of ICT (Information and Communications Technology). E-Governance is in essence the application of the information communication and technology to government functioning in order to create “Simple, Moral, Accountable, Responsive, and Transparent (SMART) governance. The revolution in Information and Communication Technology has brought a whole new agenda for governance into the realm of possibility. E-Governance comprises decisional processes and the use of ICT for wider participation of citizens in public affairs. The purpose of implementing e-governance is to improve governance processes and outcomes with a view to improve the delivery of public services to citizens. Initially, the e-governance activity starts with providing information services by the government departments to the public in terms of state websites. These websites provide information about the department concerned, its aims, objectives, organizational details, facilities available, and services provided to the public along with the fee payable etc. However, as the role of IT in the specific organization increases, the websites of government departments attempt at providing more advanced services. Gradually this e interaction of the government with the public leads to organizational transformation, transparency in disbursing public services, and increase in citizen participation in the government. However this radical move of government in achieving the goal of good governance will not be effective unless it's supported by the basic foundational mechanism which includes:

- **Connectivity,**
- **Content,**
- **Capital,**
- **Capacity,**
- **Stringent data protection laws,**
- **Digital literacy.**

E-governance can offer numerous possibilities for improving nation's public sector by responding to the basic needs of its citizen's ,but at the same time it needs a strong back end functional support to successfully maintain the e-governance initiatives, in the absence of which the system will collapse. Therefore the prime responsibility under e- governance regime lies on maintaining confidentiality, protection, and integrity to the personal data of an individual. E-government is seen as an instrument to simultaneously increase the efficiency, transparency, and accountability of public administration and improve public service delivery. Consequently, this has transformed the traditional delivery of public sector services; these developments have implications and pose challenges for privacy and security. It has become the bedrock in this contemporary era and the elementary privacy related question that arises out of this scenario is:

- Who is responsible for data identity theft?
- Who will compensate for personal data intrusion?
- Who is taking the prime responsibility for data security?
- Who is accountable to whom for any unauthorized use of personal data?

All this has become the cause of concern because while living with the digital identity, we require more security and protection to our personal data and that is not possible without stringent data protection laws.

PRIVACY IN TECHNOLOGICAL ERA

Human rights are those minimal rights individuals need to have, by virtue of being member of human family, these rights have been given paramount importance and are recognized as sacrosanct and inviolable. Among the rights privacy is the most valuable human right of all. The quest of privacy is an inherent instant of all human beings. The general idea of “private” can be conceptualized as the practices or acts which we want to protect from public scrutiny. It may be said that privacy is antithesis of being public. **Jeffery Reiman** states that privacy functions “as a means of protecting freedom, moral personality, and a rich and critical inner life”. **Alan Westin** described privacy as a “claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others”. Privacy, as a fundamental human right, cannot be limited or crippled to a few interpretations. It is a multidimensional notion that encompasses a wide range of privacy protection within its scope. The notion of privacy gained traction throughout the world as technology advanced. ICT is presently through a phase of incredibly fast development, which has broad societal implications. The most noticeable of these changes are those brought on by the internet's increasing internalization of many daily transactions. Making sense of what is actually happening with regard to one's personal information is challenging due to the pace, scale, and complexity of the developments. The persuasive hype compounds the challenge of thinking clear about these important phenomena. With the rapidly increasing growth of digitalization all over the world, the requirement for securing data privacy is high. Data Privacy sometimes referred to as informational privacy is one of the important facet of right to privacy, which has gained hype due to the technological inclusion in the processes of governance. There is no concrete definition of data privacy, however it is conceptualized as a right of an individual to know how his/her personal information is used, stored and shared with a corresponding duty upon state /any organization who is handling with the personal information to respond to those questions and manage personal data by adopting effective data privacy and security measures. According to IITF Principle of the Unites States, Information privacy is “an individual's claim to control the terms under which personal information i.e., information identifiable to the individual is acquired, disclosed, and used”

Usually, when we start something new, we might face some challenges like time management, communication, implementation, adapting to the market change competition, etc. But when a government starts some new ideas, the government faces numerous challenges. The major issue is regulatory. It's crucial to know the rules before deciding how to use the innovative technology at your disposal. When starting a particular service or idea from start to finish the regulations are most prominent. Technology cannot function independently. Citizens need to obtain the assistance they require at the lowest possible cost when needed. When tracking the progress of a project or interacting with the public, a government needs to be capable manage material swiftly and effectively. And in accomplishing that task Legal infrastructure possesses a significant impact on how the ICT infrastructure develops and grows, as well as how it affects the electronic government framework as a whole. Since legal architecture is an integral part of the e-governance program, it serves as the foundation for administration technology. The primary query that must have a positive response before any effective e-governance organization is launched is

- Are the rules and regulations required to permit and support the move towards e-governance initiatives in place?

E-governance innovations have effectively made transparency, accessibility, and efficiency in government service delivery possible. But, on the other hand, grave legal issues are also being accelerated in quite speedy digitization of public services and governmental procedures. Some serious causes include data protection, privacy, cybercrime, intellectual property, jurisdictional concerns, and enforcement methods. With the help of growing technology, legal frameworks find it hard to keep up with the rapid development or changes within an increasingly digitalized society. An adequate statutory framework is a sine qua non for successful e-governance, providing the sturdiness needed to govern and protect digital

activities within a legally sound position. The principal elements of this framework would comprise data privacy, cybercrime law, and cyber security.

A periodic and systematic review of existing regulations is important for an updated legal framework that supports the ongoing needs of e-governance. Law, adopted as fast as technology is pace-setting, can become outdated pretty quickly and may be incompetent to reply to issues such as cyber threats and data privacy concerns. The government must always evaluate the applicability and effectiveness of existing regulations and their necessity to be updated according to international requirements. Especially in data protection and security areas, adjustments are needed much earlier due to new challenges that come.

CONCLUSION

In this world, we the humans have been gifted with various inherit rights, by the nature which is invaluable and inalienable. Among them privacy is the most valuable and the most vulnerable human right in this technological driven world. The new technologies have enhanced the possibilities of invasion into the privacy of individuals and provided new tools in the hands of eavesdroppers. The digital transformation in the field of governance is leading us towards reaching the goal of good governance but it cannot be tagged as an effective and efficient mechanism unless privacy and security issues are given prime importance. Unless the balance between the electronic governance and data privacy related issues are settled down with amicable statutory laws, there would be at each step a vulnerability to the data privacy of an individual. E-governance is a transformative tool for improving government operations and client assistance, not just for developing cost-effective community amenities but also as a reforming device and a means to change the government. Thus, instead of merely competing with and attempting to imitate the practical expertise of another domain, it is important to intellectualize the objective challenges of implementing e-governance. It is difficult to imagine a success story when a nation-state is unable to categorize and choose a clear, impartial strategy for adopting and using Electronic Governance.

References

- T.M.Samuel, Maria Samuel, Information Technology and the Law , Commonwealth Publishers, 2008.
- P.Panneervel, E-Governance a Change Management Tool, Rawat Publications, 2005.
- Dr. Vasu Deva, E-Governance in India- A Reality, Commonwealth Publishers, 2005.
- C.S.Prabhu, E-Governance, Concepts, and Case Studies Prentice Hall of India Private Limited, New delhi, 2005
- Sourya Joyee De, “Privacy Policies of E-Governance Initiatives: Evidence from India”, Volume 20, Issue 4, Journal of Public Affairs May 2020.
- E-Governance in India: Concept Initiatives and Issues, by Insights IAS(Simplifying IAS preparation) available at <https://www.insightsonindia.com/2014/11/23/e-governance-india-concept-initiatives-issues/> Visited on (January 20th, 2021)
- Second Administrative Reforms Commission, Eleventh Report on Promoting E-Governance, The smart Way Forward, (December, 2008)
- Gupta, R., Pal, S.K. and Muttoo, S.K., 2020. Cyber security assessment education for E-governance systems. Innovations in Cyber security Education,
- Lokhande, M.A., 2004. E-Governance in India. Yojana, 48(12)
- Gaurav Goyal, Ravinder Kumar, “The Right to Privacy in India: Concept and Evolution” Partridge Publishing, 2016
- Jeffrey Reiman is the William Fraser McDowell Professor Emeritus of Philosophy and Social Policy
- Alan Furman Westin (October 11, 1929 – February 18, 2013) was a Professor of Public Law & Government Emeritus, Columbia University, former publisher of Privacy & American Business, and former President of the Center for Social & Legal Research
- E-Governance in India, Vishwas Tripathi, Anmol Publications Pvt.LTD, 2007