



Identifying the Dimensions, Components, and Criteria of the E-Government Legal System

Ebrahim Raana Rahbarkhah ¹, Ahmadreza Behniafar ^{2*}, Ali Pourghassab Amiri ³

¹Ph.D Student, Department of Law, Damghan Branch, Islamic Azad University, Damghan, Iran.

^{2*} Assistant Professor, Department of Law, Damghan Branch, Islamic Azad University, Damghan, Iran
(Corresponding Author).

³ Assistant Professor, Department of Law, Damghan Branch, Islamic Azad University, Damghan, Iran.

Abstract

The primary objective of this research is to identify the dimensions and components of the legal framework governing e-government. The expansion of information and communication technologies and the transformation of public service delivery methods have underscored the urgent need to re-examine the structures and criteria of the legal system governing e-government. E-government entails more than the mere digitization of government services; it requires the establishment of a coherent set of legal rules, principles, and mechanisms capable of regulating and safeguarding relationships among the government, citizens, businesses, and other stakeholders within the digital environment. This study aims to identify the dimensions and components of the e-government legal framework. Adopting an applied approach and a descriptive-analytical methodology, the research identifies and analyzes the key dimensions of this legal system through a review of legal foundations and relevant scholarly literature. The findings indicate that the e-government legal framework can be categorized into dimensions such as the legal recognition and validity of electronic documents and signatures; the protection of privacy and personal data; information security and combating cybercrime; transparency and open access to information; citizens' rights in the digital space; the liability and accountability of government agencies; the validity and admissibility of electronic evidence; the regulation of electronic relationships and transactions; equal access and the prohibition of digital discrimination; and mechanisms for oversight and the resolution of electronic disputes. Accordingly, the effectiveness of e-government is not limited to the existence of technical infrastructure; rather, it requires a comprehensive, coherent, and up-to-date legal framework that keeps pace with technological advancements. Research findings indicate that harmonizing laws, safeguarding citizens' fundamental rights, enhancing digital security and trust, and precisely defining the responsibilities of public institutions constitute key legal prerequisites for the realization of e-government.

Keywords: "E-government"; "Legal framework"; "Privacy"; "Data governance"; "Institutions active in the e-government sector."

Received: 05 Dec 2023

Received: 29 Dec 2023

Accepted: 31 Dec 2023

Introduction

E-government represents a means through which governments can employ new technologies to provide individuals with appropriate access to governmental information and services, improve the quality of public services, and create broader opportunities for participation in democratic processes and institutions. The effective implementation of e-government also contributes to the establishment of a transparent, accountable, and trust-based environment. By enhancing transparency in information and communications through the application of new information technologies, e-government can be regarded as an unparalleled strategy for strengthening the rule of law and reducing administrative corruption (Pour Esmaeil et al., 2025).

With the rapid expansion of emerging technologies, particularly artificial intelligence, significant transformations have occurred across various dimensions of human life. Despite the numerous benefits and opportunities offered by these technologies, concerns have also emerged regarding potential violations of individuals' privacy, which may have substantial legal, social, and ethical consequences (Khan, 2025).

One of the most fundamental challenges within the legal framework of e-government is the inadequate protection of individuals' privacy. Privacy is among the rights upon which individuals depend because of their personal needs, while, at the same time, the requirements of collective life oblige members of society to recognize and respect this right in relation to others. In addition to encompassing a substantial portion of interactions between natural and legal persons and governmental institutions, e-government can positively affect individuals' daily lives, strengthen their interaction with governance, transform citizens from passive consumers into active participants, improve service-delivery processes across various sectors, reduce the distance between citizens and public officials, and promote social justice by creating equal opportunities for all members of society. These characteristics make the establishment of e-government increasingly indispensable.

Accordingly, a fundamental challenge lies in developing mechanisms for establishing and effectively implementing e-government. In this regard, based on the laws and regulations governing society, it is necessary to establish transparency and governmental accountability as core principles and to facilitate meaningful citizen participation in public affairs. Good governance depends upon informed and knowledgeable citizens; therefore, within the framework of e-government, citizens should be provided with opportunities for maximum and effective participation. Another important issue concerns the potential conflict between freedom of expression and access to information, on the one hand, and the right to privacy, on the other. The present study therefore seeks to determine, through legal analysis and in light of the degree of transparency established under national legislation, the extent to which the legislature has protected individuals' privacy within the context of e-government and what legal framework governs such protection. The ultimate objective is to identify an appropriate approach to safeguarding this individual value without allowing individuality to be subordinated to the collective conscience, while also developing recommendations for achieving an appropriate balance between these two important values.

On the other hand, because of the public-service nature of e-government, a balance must be maintained between efficiency and privacy. Governments require access to information in order to provide accurate and effective services; however, the principle of necessity requires that only information that is genuinely necessary be collected. This balance is particularly important in areas such as healthcare, taxation, social security, education, civil registration, and welfare services (Guo, 2024).

One of the most significant issues is the integration of information databases. Interconnecting systems can reduce the burden on citizens and prevent the repeated submission of documents; at the same time, however, it may increase the possibility of creating comprehensive profiles of individuals. Accordingly, technical interoperability must be accompanied by legal safeguards, ensuring that every data exchange has a clearly defined purpose, legal authorization, recipient, and scope. Another issue concerns transparency. Citizens should, to the greatest extent possible, be informed about which governmental agency receives their data, the purposes for which the data are processed, and the circumstances under which the data may be transferred to another agency. Such transparency is essential for public trust. Indeed, digital government cannot achieve sustainable maturity without citizens' trust. The right to challenge and review decisions must also be guaranteed. If a decision that significantly affects a citizen's legal or economic status is made on the basis of inaccurate data or a defective algorithm, the citizen must have an effective opportunity to challenge the decision and seek correction. This principle has become increasingly important in the era of automated decision-making (Shabanian, 2023).

Review of the Theoretical Foundations

The Concept of the Legal System

A legal system can be understood as a network of formal rules and interconnected institutions established within a society for the recognition, interpretation, implementation, and enforcement of rights and obligations. This concept is broader than the notion of “law” itself, because legislation constitutes only one component of a legal system. Other components include courts, administrative institutions, legal professions, judicial practice, dispute-resolution mechanisms, and legal culture (Merryman & Pérez-Perdomo, 2019).

The Concept of E-Government

E-government should not be understood merely as the transfer of administrative services from face-to-face environments to online platforms. Rather, it refers to a transformation in the way public services are designed, delivered, and governed; the reconfiguration of organizational processes; interactions between governments, citizens, and businesses; the use of data and technology; and, ultimately, the transformation of the relationship between public institutions and society (Wirtz, 2022).

Accordingly, the success of e-government cannot be reduced to the existence of a website or electronic system. Instead, it depends on a combination of institutional, managerial, technological, legal, and social capacities. Contemporary literature on digital governance also emphasizes the transition from “e-government” toward “digital governance,” in which data, platforms, artificial intelligence, interoperability, and stakeholder participation are placed at the center of public-service design (UN DESA, 2024).

The study by Dehnoor (2026), adopting a descriptive-analytical approach and drawing upon library resources, legal documents, and scholarly articles, examines the concept of digital governance and analyzes the public-law challenges arising from the implementation of e-government in Iran. The findings indicate that the major challenges include the absence of a comprehensive personal data protection framework, incomplete implementation of the principle of transparency, ambiguity concerning the accountability of administrative institutions, the persistence of the digital divide, and limitations on judicial oversight of electronic administrative decisions. The study concludes that achieving effective digital governance in Iran requires the enactment of comprehensive data-protection legislation, strengthening transparency and accountability mechanisms, updating judicial review mechanisms, and adopting effective policies to safeguard citizens’ rights in the digital environment.

The study by Shojaei and Rahmani (2026), using a descriptive-analytical approach, examines privacy-protection challenges in the United States, the European Union, and Iran. In the United States, the legal framework for privacy protection is based on legislation such as the Privacy Act of 1974 and the Children’s Online Privacy Protection Act (COPPA), with an emphasis on self-regulation and the role of the private sector. However, the absence of regulatory coherence and heavy reliance on voluntary mechanisms have generated implementation challenges. By contrast, the European Union, through the General Data Protection Regulation (GDPR), has established a comprehensive and stringent framework based on principles such as transparency, consent, and the right to erasure. In Iran, although Articles 22 and 25 of the Constitution and legislation such as the Computer Crimes Law and the Electronic Commerce Law provide fragmented forms of privacy protection, the absence of comprehensive legislation, regulatory fragmentation, and weak oversight remain major challenges. The findings emphasize the importance of employing protective technologies such as encryption and digital identity management, as well as strengthening user education and cooperation between governmental and civil-society institutions to enhance data protection.

The study by Shirzaei et al. (2025), adopting a descriptive approach, examines the major cybersecurity challenges facing new-generation e-governments and proposes legal and managerial mechanisms for addressing these challenges. The findings indicate that these challenges can be classified into three levels: technical-technological, managerial-institutional, and legal-legislative. At the legal level, the inefficiency of existing legislative frameworks, weak coordination among responsible institutions, and the absence of specialized judicial procedures constitute major obstacles. At the managerial level, the lack of comprehensive risk-management strategies, weaknesses in information-security governance, and shortages of specialized human resources represent fundamental challenges. The study ultimately

proposes measures such as developing an integrated legal framework, establishing a risk-based security-management system, and designing a participatory cybersecurity governance model in order to provide an effective framework for securing next-generation e-government systems.

Research Method

An inductive analysis based on theoretical foundations was employed to examine the role of the legal system of e-government in protecting individuals' privacy and to identify, analyze, and report patterns emerging from the qualitative research data. The research data were analyzed using a qualitative inductive analysis approach grounded in theoretical foundations, with the assistance of **MAXQDA** software. The qualitative data obtained through interviews with experts were analyzed in order to identify the research variables and criteria.

Research Findings

Thematic Analysis Process

The analysis process was conducted at four levels. First, meaningful units related to law, digital government, and privacy were identified. Second, conceptual labels were assigned to the relevant statements. Third, closely related codes were integrated into sub-themes. Fourth, the relationships among the three major themes were interpreted.

At this stage, items that appeared within two domains were not eliminated; rather, they were assigned to the appropriate category based on their conceptual function. For example, cybersecurity constitutes both a component of the legal system and a prerequisite for the effective protection of privacy within e-government.

The coding results indicate that the three research variables do not have a simple linear and independent relationship. The **legal system** establishes the rules and legitimate boundaries of action; **e-government** provides the technological and operational environment through which those rules are implemented; and **individual privacy** represents one of the most important domains in which the tangible consequences of this relationship become evident.

Accordingly, the central theme derived from the analysis can be designated as "the capacity of the legal system to safeguard individuals' rights throughout the process of government digitalization."

Table 1. Thematic Analysis of the Main Variables, Subthemes, Axial Codes, and Coding Frequency

Main Variable	Subtheme	Axial Codes	Frequency
Legal System	Comprehensiveness and Coherence of Rules	Existence of a legal basis; coordination of laws; determination of jurisdiction; enforceability	26
Legal System	Accountability and Responsibility	Attribution of decisions; organizational responsibility; oversight; enforcement mechanisms	21
Legal System	Data Protection and Citizens' Rights	Privacy; access; rectification; objection; limitations on use	24

Legal System	Flexibility and Technology Regulation	Risk-based regulation; technology neutrality; response to emerging technologies	17
E-Government	Digitization of Services	Online services; reduction of in-person visits; redesign of government processes	18
E-Government	Integration and Interoperability	System connectivity; digital identity; data exchange	23
E-Government	Data-Driven Governance and Intelligentization	Data analytics; algorithms; proactive services; digital decision-making	19
E-Government	Public Value and User-Centeredness	Trust; justice; service quality; participation; citizen experience	20
Individual Privacy	Individual Control and Agency	Awareness; consent; access; rectification; objection; deletion	22
Individual Privacy	Data Life Cycle and Data Limitation	Data minimization; purpose limitation; retention; secondary use	25
Individual Privacy	Security and Protection-Oriented Architecture	Confidentiality; integrity; availability; Privacy by Design	24
Individual Privacy	Contextual Privacy	Proportionality of data flows to context; roles; purpose; recipient	18

Interpretation of the First Concept: The Legal System

Thematic analysis demonstrates that the **“legal system”** in this study should not be understood merely as a collection of existing laws. Rather, it constitutes a multilayered structure encompassing rules, institutions, jurisdictions, oversight mechanisms, and enforcement mechanisms. This interpretation is consistent with Kelsen’s approach to the hierarchy of norms, Hart’s distinction between primary and secondary rules, and the institutional approach to law.

In the digital environment, the existence of a legal provision becomes meaningful only when the competence of the relevant institution, the method of implementation, the allocation of responsibility, and the availability of dispute-resolution mechanisms are also clearly defined. The theme of **“comprehensiveness and coherence of rules”** carries the greatest weight among the identified legal themes. This finding indicates that the principal challenge of digital law is not the absence of a single statute, but rather the fragmentation of legal rules and the need for coordination among legislation, regulations, technical standards, and implementing guidelines.

The sources reviewed also identify governmental data law as encompassing a range of rules concerning access, reuse, privacy, and intellectual property. Accordingly, the regulation of the relationship between government and data cannot be reduced to a single legislative instrument.

The second theme is **“accountability and responsibility.”** Digitalization may distribute responsibility among administrative officials, government agencies, technology contractors, and automated systems. Therefore, the thematic analysis indicates that the greater the role of technology in decision-making, the greater the need for clear rules governing attribution of responsibility and human review. From Hart’s perspective, this issue relates to secondary rules concerning competence, modification, oversight, and dispute resolution.

The third theme is **“data protection and citizens’ rights.”** A legal system can effectively protect privacy only when rules governing data collection, processing purposes, access, rectification, sharing, and secondary use are clearly established. Consequently, at the analytical level, privacy should not be regarded as a secondary outcome of information technology law; rather, it constitutes one of the principal criteria for assessing the effectiveness of a digital legal system.

The fourth theme is **“flexibility and technology regulation.”** The rapid pace of technological change means that highly detailed regulations tied to specific technologies may have a relatively short lifespan. The principle of **technology neutrality** and **risk-based regulation** are among the mechanisms capable of reducing the gap between innovation and law. This finding is also consistent with Lessig’s approach, according to which the regulation of digital behavior does not occur exclusively through legal rules; rather, system architecture itself possesses regulatory capacity.

The overall interpretation of this theme is that a digital legal system becomes effective when it moves from **“issue-specific legislation”** toward **“technology-oriented legal governance.”** Issue-specific legislation may establish rules concerning the validity of electronic signatures, cybercrime, or a particular digital service. However, a data-driven government encounters interconnected and interdisciplinary challenges. Accordingly, the coherence of rules, allocation of jurisdiction, accountability, and adaptability to emerging technologies become more important than the sheer number of laws.

This conclusion is consistent with the research gap identified in the underlying literature, which emphasizes assessing the **functional performance of law in technology governance**, rather than merely counting the number of regulations.

Interpretation of the Second Concept: E-Government

With respect to the **e-government** variable, thematic analysis demonstrates that e-government has evolved from a primarily technical concept into an institutional one. At the initial stage, technology was largely employed to provide information and online services. With the emergence of **digital government**, however, data and technology have become integrated into policymaking, service design, implementation, monitoring, and evaluation.

The OECD framework similarly describes this transformation through concepts such as **digital by design, a data-driven public sector, government as a platform, openness by default, user-driven approaches, and proactiveness.**

The theme of **“integration and interoperability”** carries considerable weight. The reason is straightforward: when government agencies move from isolated systems toward shared infrastructures, administrative efficiency increases, while at the same time the flow of data across organizations becomes more extensive. Accordingly, interoperability without clearly defined purposes, legal authorization, access levels, and responsibility may lead to excessive concentration of data. This duality has also been identified in the underlying literature as one of the central challenges of digital government.

The theme of **“data-driven governance and intelligentization”** demonstrates that governmental transformation does not simply involve converting paper-based forms into online forms. Once data analytics, artificial intelligence, and algorithmic decision-making become integrated into public

administration, new legal issues emerge concerning **explainability, data errors, bias, attribution of responsibility, and human oversight**. Therefore, the maturity of digital government cannot be achieved without corresponding maturity in legal and oversight mechanisms.

The findings concerning the theme of “**public value and user-centeredness**” likewise demonstrate that the success of e-government should not be measured solely by the number of digital systems or the extent to which services are available online. Equal access, trust, transparency, accountability, and citizens’ experiences constitute important components of the actual value generated by digital transformation. The underlying literature has similarly highlighted potential tensions between user-centeredness and public values such as justice and equality.

The interpretation of these findings indicates that, at an advanced stage of maturity, e-government constitutes a “**governance infrastructure**” rather than an information technology project. As government becomes increasingly data-driven and integrated, the role of law in defining the boundaries of data flows, organizational responsibility, and citizens’ rights becomes increasingly significant.

Consequently, the relationship between e-government and the legal system is **bidirectional**: law must facilitate digital transformation, while digital transformation confronts the legal system with new questions concerning automated decision-making, digital identity, interoperability, and other emerging technologies.

Interpretation of the Third Concept: Individuals’ Privacy

With respect to the **individual privacy** variable, four prominent subthemes emerged: **individual control and agency, the data life cycle, security and privacy-by-design architecture, and contextual privacy**. This structure is consistent with the existing literature in the underlying research, which examines privacy across four domains: users, data and information, cybersecurity, and information technology.

The theme of “**individual control and agency**” demonstrates that citizens should not be treated merely as objects of data processing. Awareness of data collection, the ability to access and rectify personal data, the right to object, and, where legally applicable, the right to request deletion constitute important indicators of individual agency.

Nevertheless, the analysis indicates that **consent alone is insufficient**. In the context of public services, citizens may have no genuine alternative if they wish to obtain a particular service. Accordingly, the principles of necessity, proportionality, and purpose limitation should operate alongside consent.

The theme of the “**data life cycle**” demonstrates that privacy violations may occur at any stage, from data collection to deletion. Accordingly, the principles of **purpose limitation, data minimization, accuracy, storage limitation, and control over data sharing** are of particular importance.

The documentary analysis further demonstrates that **inferred data** have blurred the distinction between information directly provided by an individual and information that a system derives from observing or analyzing that individual’s behavior.

The theme of “**security and privacy-by-design architecture**” demonstrates that privacy cannot be sustainably protected without technical security. At the same time, technical security cannot substitute for the legal legitimacy of data processing. Confidentiality, integrity, and availability, on the one hand, and **privacy by design**, on the other, must be accompanied by appropriate legal rules.

This finding is supported by the underlying literature concerning the necessity of incorporating data protection into the architecture and default settings of digital systems.

“**Contextual privacy**” represents the most significant interpretive level of the findings. According to the theory of **contextual integrity**, the central question is not merely whether particular information qualifies as personal data. Rather, it must be determined **who** receives the data, **what data** are involved, **from whom** they are obtained, **for what purpose** they are processed, and **under which rules** the transfer takes place.

Accordingly, the transfer of a citizen's data from one government agency to another may be technically feasible; however, if such transfer is incompatible with the original purpose and context in which the information was collected, it may raise significant privacy concerns.

The overall interpretation of these findings is that privacy in digital government is not a “**static right**”, but rather a **governance process for regulating the flow of information**. This conclusion is consistent with the historical evolution of the concept of privacy—from the right to be left alone, to informational self-determination and control over personal information, and subsequently toward contextual approaches to privacy.

Therefore, privacy assessment should simultaneously address **three levels: individual rights, the data life cycle, and technological architecture**. Eliminating any one of these dimensions would result in an incomplete understanding of the actual state of privacy protection.

Table 2. Analysis of the Relationship among the Three Main Variables

Relationship Mechanism	Analytical Result
Legal System → E-Government	Determines jurisdiction, validity, responsibility, data rules, and the possibility of objection; establishes the legitimate scope of digital transformation.
E-Government → Individual Privacy	Expansion of data collection, integration, and analysis; digital transformation creates both opportunities for improved services and risks arising from data concentration.
Legal System → Individual Privacy	Determination of rights, duties, purpose limitation, and enforcement mechanisms; effective privacy protection depends on the coherence and enforceability of rules.
Individual Privacy → Trust	Data control, security, transparency, and the right to object; data protection is one of the foundations of citizens' trust in digital government.
Interoperability → Individual Privacy	Inter-organizational data sharing increases efficiency, but without access controls, the risk of privacy violations increases.

Interpretive Synthesis of the Findings

From an interpretive perspective, the most significant finding of the study is that the three variables cannot be analyzed independently of one another. The **legal system** establishes the normative framework; **e-government** implements that framework through digital architecture and processes; and **privacy** represents the point at which the consequences of such implementation become evident in terms of individual rights. Accordingly, weaknesses in any one of these three dimensions can undermine the effectiveness of the other two.

Conclusion

Digital transformation in governance structures has fundamentally altered the concept of government and the nature of interactions between governments and citizens. E-government represents one of the most significant manifestations of this transformation and has emerged with the objective of enhancing the speed, transparency, accessibility, efficiency, and accountability of public services. Nevertheless, the

effective realization of e-government cannot be achieved merely through the development of information technology infrastructure and the establishment of electronic systems. Rather, it requires a comprehensive legal system capable of defining the relationships, rights, obligations, and responsibilities of actors operating within the digital environment. From this perspective, law must evolve in parallel with technological developments and provide the necessary framework for legitimacy, security, trust, and accountability in the electronic environment.

The findings of this study demonstrate that the **legal system of e-government is multidimensional** and cannot be confined to a particular branch of law. One of its most important dimensions concerns the recognition of the legal validity of electronic documents, data, and signatures. When administrative decisions, contracts, correspondence, and records are created and exchanged in digital environments, the legal system must clearly determine the requirements for their validity, authenticity, integrity, and admissibility as evidence. The absence of such a framework may undermine public confidence in electronic services and increase the likelihood of legal disputes.

Another important dimension is the **protection of citizens' privacy and personal data**. Because e-government involves the collection, processing, and storage of substantial amounts of citizens' information, it raises significant questions concerning the manner of data collection, the purposes for which data are used, retention periods, access by different individuals and institutions, and mechanisms for protecting information. Accordingly, an effective legal system must not only enable the legitimate use of data by government authorities for the provision of public services but also establish clear limits on interference with individuals' privacy and provide appropriate safeguards against the misuse or unauthorized disclosure of information.

Information security and combating cybercrime also constitute fundamental components of the legal criteria governing e-government. The increasing dependence of public services on digital systems exposes governments to threats such as unauthorized access, theft or destruction of data, electronic forgery, cyberattacks, and disruption of public services. Therefore, the legal system must not only clearly define unlawful conduct in cyberspace but also establish the responsibilities of individuals and institutions, security requirements, and mechanisms for prevention, detection, investigation, adjudication, and compensation for damages.

From another perspective, **transparency and access to information** constitute among the most important legal functions of e-government. Digital technologies can facilitate faster access by citizens to public information, laws, regulations, governmental decisions, and public services. However, such transparency must operate within a clearly defined legal framework that simultaneously guarantees citizens' right of access to public information and prevents the disclosure of confidential information, personal data, and information whose disclosure could adversely affect individual rights or public interests.

Another fundamental finding of the study concerns the **recognition and protection of citizens' rights in the digital environment**. Citizens in an e-government system are not merely recipients of services; they are rights-holders whose rights must be respected throughout all stages of their digital interactions with public authorities. Equal access to services, the right to be informed about the processing of personal information, the right to challenge administrative decisions, the right to information security, and access to effective complaint-handling mechanisms are among the rights that should be incorporated into the legal framework of e-government.

Furthermore, **the responsibility and accountability of government agencies** constitute a fundamental criterion of the legal system of e-government. The use of automated systems and technology-based processes should not create ambiguity regarding the legal responsibility of public authorities. It must be clearly established which individual or institution bears responsibility in cases involving errors, violations of citizens' rights, unauthorized disclosure of information, or erroneous decision-making within electronic processes. Accordingly, e-government requires clear rules concerning administrative and civil liability and, where appropriate, criminal responsibility.

Equal access and the prevention of digital discrimination constitute another important component. The digitalization of public services can contribute to administrative and social justice only when all citizens have a meaningful opportunity to benefit from such services. Differences in access to the Internet, technological resources, digital skills, or electronic services should not result in the exclusion of particular groups from public rights and services. Therefore, e-government policy should not only promote the expansion of digital services but also provide mechanisms to support individuals who, for various reasons, are unable to make effective use of electronic services.

Overall, the criteria of the legal system of e-government are formed through an **interconnected network of legal, institutional, and protective components**. The legal validity of electronic interactions cannot be sustained without information security; security cannot ensure public trust without effective privacy protection; and the provision of electronic services without transparency, accountability, and guarantees of citizens' rights may undermine public confidence. Accordingly, the legal system of e-government must adopt a comprehensive and coordinated approach that balances administrative efficiency, security requirements, fundamental citizens' rights, and the imperatives of digital transformation.

On this basis, the **optimal legal framework for e-government** should rest upon several fundamental principles: first, updating legislation in accordance with technological developments; second, harmonizing fragmented laws and regulations governing electronic services and transactions; third, strengthening legal protections for privacy and personal data; fourth, clearly defining the responsibilities of executive agencies and digital-service providers; fifth, ensuring the security and trustworthiness of governmental systems; sixth, guaranteeing equal access to public services; and seventh, establishing effective mechanisms for oversight, complaint resolution, and compensation for damages.

Ultimately, it can be concluded that the **success of e-government depends not merely on the extent of technological development but, more fundamentally, on the quality and coherence of its legal framework**. An effective legal system must facilitate innovation and the digitalization of public services while safeguarding citizens' rights and freedoms and clearly defining the responsibilities of government and other actors within the digital environment. Therefore, identifying and organizing the dimensions and components of the legal criteria governing e-government can provide a basis for assessing the existing situation, identifying legislative gaps, and designing a more comprehensive legal framework for digital governance.

References

1. Shabanian, S. (2023). *E-Government*. Andisheh Asr Publishing.
2. Pour Esmaeil, R., Partovi, A., & Zolqadr, M. (2025). The impact of e-government on the rule of law and transparency in Iran and Malaysia. *Quarterly Journal of Political Research in the Islamic World*, 15(2).
3. Khan, Y. (2025). The impact of artificial intelligence on individuals' privacy from the perspective of the Iranian legal system. *10th International Conference on Jurisprudence, Law, Psychology, and Educational Sciences in Iran and the Islamic World*.
4. Dehnoor, S. (2026). *Digital governance and public-law challenges in Iran: An examination of citizens' rights in e-government*. [Scientific Report].
5. Shojaei, A. S., & Rahmani, S. (2026). Legal framework for privacy protection in the digital environment: A comparative study of the legal systems of the United States, the European Union, and Iran. *Quarterly Journal of Comparative Legal Research*, 30(2).
6. Shirzaei Dalir, F., Brahouei, S., Rigi, S., Nourzaei, Y., & Khadem Astaneh, A. M. (2025). Cybersecurity challenges in next-generation e-governments and legal-managerial solutions. *6th International Conference on Political Science, Management, Economics, and Accounting*.
7. Cho, G. (2023). *Information technology law in Australia*. Kluwer Law International.
8. Merryman, J. H., & Pérez-Perdomo, R. (2019). *The civil law tradition: An introduction to the legal systems of Europe and Latin America* (4th ed.). Stanford University Press.

9. UN DESA. (2024). United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development. United Nations.
10. Wirtz, B. W. (2022). Digital government: Strategy, government models and technology. Springer.