How to cite this article:
Samizadeh, M. H., Dashti, M. T., & Ebrahimian, H. (2026). Barriers to the Implementation of E-Governance in the Iranian Legal System. *Journal of Historical Research, Law and Policy, 4*(3), 1-17. https://doi.org/10.61838/jhrlp.251

Article history:
Original Research

Dates:
Submission Date: 12 November 2025
Revision Date: 10 February 2026
Acceptance Date: 17 February 2026
First Pubication Date: 24 February 2026
Final Pubication Date: 01 May 2026

Barriers to the Implementation of E-Governance in the Iranian Legal System

1. Mohammad Hasan. Samizadeh[1] : Department of Public Law, Qo.C., Islamic Azad University, Qom, Iran
2. Mohammad Taghi. Dashti[2*]: Associate Professor, Imam Baqir University, Tehran, Iran
3. Hojjatollah. Ebrahimian[3]: Department of Public Law, Qo.C., Islamic Azad University, Qom, Iran

*corresponding author's email: Mohammadtaghi.dashti@iau.ir

ABSTRACT

Despite sustained policy attention and repeated legal references, e-governance in Iran has not achieved effective, coherent, or transformative implementation. This article examines the causes of this failure by shifting the analytical focus from prerequisites and ideal conditions to the structural barriers that actively obstruct digital governance in practice. Adopting a doctrinal legal analysis combined with institutional critique, the study conceptualizes e-governance as a legal–institutional mode of exercising public authority rather than a purely technological innovation. The analysis demonstrates that the absence of a comprehensive e-governance law has produced a fragmented normative framework characterized by legal dispersion, regulatory ambiguity, and weak enforceability. These legislative deficiencies are reinforced by institutional barriers, including the lack of a central coordinating authority, bureaucratic resistance, and regulatory overload at the executive level, all of which contribute to policy incoherence and implementation paralysis. Judicial barriers further undermine e-governance through the absence of a developed doctrine of digital evidence, formalistic interpretation of digital rights, limited judicial specialization, and weak oversight of state-operated digital platforms. In parallel, participatory and societal barriers—such as state-centric digital design, digital inequality, and pervasive trust and privacy concerns—restrict meaningful citizen engagement and exacerbate legitimacy deficits. Taken together, these barriers reveal that e-governance in Iran has been approached primarily as a technical and managerial project, while its legal, institutional, and judicial foundations remain underdeveloped. The article concludes that without removing these structural barriers, digital initiatives will continue to function symbolically rather than substantively, perpetuating the gap between legal recognition and effective governance.

Keywords: *E-governance; digital governance; public law; legal barriers; administrative law; Iran*

Introduction

The rapid expansion of digital technologies over the past few decades has fundamentally altered the way public power is exercised, administered, and legitimized. Digital transformation in the public sector is no longer limited to improving administrative efficiency or accelerating service delivery; rather, it has reshaped the normative foundations of governance itself. E-governance has emerged within this broader transformation as a model that reconfigures the relationship between the state, citizens, and public institutions by embedding decision-making, service provision, and oversight within digitally mediated processes. Scholars have emphasized that this transformation is not merely technical but deeply institutional, affecting how authority is structured, accountability is enforced, and public values are realized in practice (1). In this sense, e-governance represents a shift in the architecture of public power, where information flows, data infrastructures, and algorithmic systems increasingly shape governmental action.

The move from traditional bureaucracy to digitally mediated governance has involved a gradual erosion of hierarchical, paper-based administrative models in favor of networked, data-driven systems. Classical bureaucratic governance relied on formal procedures, written records, and clearly demarcated chains of authority, features that were designed to ensure predictability and legality but often resulted in rigidity and opacity. Digital governance models, by contrast, emphasize interoperability, real-time data exchange, and cross-organizational coordination, thereby challenging the organizational silos that characterized earlier administrative systems (2). This transition has been described as a move toward “digital-era governance,” in which public administration is reorganized around integrated digital platforms rather than discrete bureaucratic units (3). Such a shift alters not only how governments operate but also how citizens interact with public authority, increasingly engaging through online portals, automated procedures, and algorithmically informed decisions.

A crucial distinction in the literature on e-governance concerns the difference between technological deployment and legal institutionalization. While many governments have adopted digital tools such as online service platforms, electronic databases, and automated decision-support systems, the mere presence of technology does not in itself constitute e-governance. Legal scholars have argued that e-governance only materializes when digital practices are embedded within a coherent legal framework that defines responsibilities, safeguards rights, and establishes mechanisms of accountability (4). Without such institutionalization, digital tools risk functioning as ad hoc administrative instruments rather than as components of a legally structured governance model. The concept that “code is law,” famously articulated to highlight how technological architectures can regulate behavior, underscores the necessity of aligning digital systems with legal norms to prevent the unchecked exercise of power through technical means (5).

In the Iranian legal system, the discourse on e-governance exists in a fragmented and often implicit form. Unlike some jurisdictions that have enacted comprehensive digital governance statutes, Iran lacks an explicit and unified statutory definition of e-governance. Instead, references to digital administration, transparency, information access, and electronic services are dispersed across constitutional principles, ordinary legislation, and policy-oriented documents. This absence of a consolidated legal concept has significant implications, as it leaves the scope, objectives, and legal consequences of e-governance largely undefined. Comparative research indicates that such definitional ambiguity often leads to inconsistent implementation and weak accountability, as administrative bodies operate without a shared legal understanding of their digital obligations (6).

Constitutional principles in Iran provide a normative foundation that could support e-governance, particularly through commitments to transparency, accountability, and public participation. However, these principles are framed in abstract terms and do not explicitly address the digital context. Ordinary laws and sector-specific regulations introduce electronic mechanisms in areas such as commerce, communication, or administrative procedures, yet they do so without integrating these mechanisms into a unified governance framework. Policy documents and strategic plans further emphasize digital transformation and smart government initiatives, but their legal status is often ambiguous, and their enforceability remains limited. International studies suggest that when digital governance relies heavily on policy instruments rather than binding legal norms, implementation tends to be uneven and vulnerable to institutional resistance (7).

This fragmented legal landscape has produced a paradoxical situation in Iran: formal acknowledgment of digital governance objectives coexists with persistent practical dysfunction. On paper, digital transformation is recognized as a desirable goal, aligned with global trends and articulated in strategic visions. In practice, however, the absence of legal coherence has resulted in overlapping mandates, unclear lines of responsibility, and weak enforcement mechanisms. Similar patterns have been observed in other contexts where digital reforms outpace legal adaptation, leading to what has been described as “digital façade governance,” in which technological adoption masks underlying structural deficiencies (8). In Iran, this paradox is further intensified by institutional complexity and a strong tradition of centralized administrative control, which complicates the integration of networked digital models.

Much of the existing discourse on e-governance in Iran and comparable systems is dominated by discussions of requirements, prerequisites, and ideal conditions for successful implementation. While such analyses highlight important normative aspirations, they often obscure the concrete obstacles that impede realization in practice. A barrier-focused approach offers a different normative lens, one that prioritizes the identification of structural constraints, legal gaps, and institutional resistances that actively undermine e-governance. Scholars of public administration have argued that reform efforts frequently fail not because goals are unclear, but because obstacles are insufficiently analyzed and addressed (9). From this perspective, a negative legal analysis centered on barriers provides a more realistic foundation for understanding implementation failure.

The predominance of “what should exist” over “what obstructs” in Iranian legal and policy discourse reflects a broader tendency toward aspirational norm-setting without corresponding enforcement capacity. Legal inflation occurs when numerous principles, policies, and programs are articulated without the institutional means to ensure compliance. In the digital governance context, this can result in a proliferation of platforms and initiatives that lack legal clarity or sustainability. International research on open government and digital transparency has shown that ambitious normative commitments often falter when they encounter entrenched administrative practices and weak sanctioning mechanisms (10). By shifting analytical focus to barriers, it becomes possible to assess how legal norms interact with institutional realities, rather than assuming linear progress from norm adoption to implementation.

The risks associated with norm inflation are particularly acute in systems where enforcement mechanisms are underdeveloped or inconsistently applied. Without clear legal consequences for non-compliance, digital governance obligations may be treated as optional or symbolic. This dynamic undermines public trust, as citizens encounter discrepancies between official rhetoric and lived administrative experience. Studies on accountability emphasize that transparency and participation only generate public value when supported by credible enforcement and oversight structures (11). A barrier-oriented analysis thus serves not only an explanatory function but also a normative one, highlighting the conditions under which legal commitments can regain credibility.

Against this background, the present study is guided by a central research question: why has e-governance failed to be effectively implemented in Iran despite repeated legal recognition and policy emphasis? Addressing this question requires moving beyond descriptive accounts of digital initiatives to examine the underlying legal and institutional dynamics that shape their outcomes. The scope of the research is deliberately limited to barriers, understood as factors that hinder or distort the realization of e-governance within the Iranian legal system. These barriers are examined across four interrelated dimensions: legal, institutional, judicial, and participatory.

Methodologically, the study adopts a doctrinal legal analysis combined with institutional critique. Doctrinal analysis is employed to examine how existing legal texts, principles, and interpretations structure digital governance, drawing on comparative insights from the broader literature on public law and digital government (12). Institutional critique complements this approach by analyzing how administrative practices, organizational cultures, and power relations affect the application of legal norms in practice. Research on street-level bureaucracy demonstrates that implementation is often shaped by discretionary decisions at the operational level, where formal rules interact with informal norms and constraints (13). This insight is particularly relevant in the digital context, where frontline administrators mediate between technological systems and legal obligations.

The study does not seek to propose a comprehensive model of ideal e-governance or to enumerate technical prerequisites for digital transformation. Instead, it aims to provide a systematic analysis of why existing efforts have fallen short, situating Iranian experience within the broader theoretical debates on digital government and public management (14). By focusing exclusively on barriers, the research contributes to a more critical understanding of e-governance, one that recognizes digital transformation as a contested and legally mediated process rather than an inevitable outcome of technological progress (15). This analytical orientation lays the groundwork for subsequent sections, which examine specific categories of barriers in detail and assess their cumulative impact on the prospects for effective e-governance in Iran.

Conceptual and Theoretical Framework of E-Governance Barriers

E-Governance as a Legal–Institutional Phenomenon

E-governance is often introduced in policy discourse as an extension of information and communication technologies into the public sector, yet such a description captures only its most superficial dimension. At a deeper level, e-governance represents a transformation in the way public authority is constituted, exercised, and constrained. Rather than functioning merely as a set of digital tools for administrative efficiency, e-governance restructures the modalities through which state power is exercised, embedding decision-making, service delivery, and oversight within digitally mediated processes. Scholars have emphasized that this transformation affects the institutional logic of governance, reshaping relationships among public agencies, citizens, and private actors (1). In this sense, e-governance must be understood as a legal–institutional phenomenon, one that alters the normative environment in which public authority operates rather than simply modernizing existing procedures.

Viewing e-governance through a legal–institutional lens highlights its intimate connection with foundational principles of public law. The rule of law, traditionally associated with legality, predictability, and the subjection of public power to legal norms, acquires new dimensions in a digital environment. Digital systems can enhance legal certainty by standardizing procedures and reducing discretionary variation, yet they can also obscure decision-making processes when algorithmic logic replaces transparent reasoning (4). Transparency, similarly, is transformed by digital governance, as information can be disseminated widely and rapidly, but only when legal frameworks compel disclosure and regulate exceptions (12). Accountability, which depends on the ability to trace decisions to identifiable actors, faces new challenges when automated systems distribute responsibility across technological infrastructures and organizational units (11). Participation, often cited as a promise of e-governance, requires more than access to online platforms; it demands legal recognition of participatory rights and procedures that ensure citizen input has normative significance (16).

Understanding e-governance as a mode of exercising public authority also underscores the importance of institutional design. Digital governance initiatives reorganize administrative structures around data flows, interoperability, and cross-agency coordination, moving away from siloed bureaucratic arrangements (17). This reorganization challenges traditional assumptions about hierarchy and control, as authority is increasingly exercised through networks rather than linear chains of command. The legal institutionalization of these networks is therefore critical, as it determines how power is allocated, how conflicts are resolved, and how rights are protected. Without such institutionalization, digital governance risks operating in a normative vacuum, where technological capability outpaces legal oversight (5).

Typology of Barriers in Public Law

A comprehensive understanding of e-governance failure requires a structured typology of barriers that captures the multifaceted nature of obstruction within public law. One category of barriers arises at the normative level, where legal frameworks fail to provide coherent, enforceable rules governing digital governance. Normative barriers include the absence of comprehensive legislation, inconsistencies among existing norms, and vague legal mandates that leave administrative bodies uncertain about their obligations. Research on digital government has shown that fragmented legal frameworks undermine coordination and weaken accountability, as agencies interpret norms selectively or prioritize competing legal requirements (6). In such contexts, the law's guiding function is diluted, and digital initiatives become discretionary rather than obligatory.

Institutional–administrative barriers constitute a second category, reflecting the organizational and managerial constraints that impede the translation of legal norms into practice. Even when laws authorize or encourage digital governance, administrative structures may resist change due to entrenched routines, professional cultures, or resource constraints. Studies of public management reform emphasize that institutions are not neutral conduits for policy implementation but are shaped by power relations and historical trajectories (8). In digital governance, institutional barriers often manifest as fragmented authority, lack of coordination among agencies, and resistance from officials who perceive transparency and automation as threats to discretionary power (3). These barriers illustrate how legal norms interact with institutional realities in ways that can neutralize reform efforts.

Judicial barriers form a third dimension of obstruction, rooted in the courts' role as interpreters and enforcers of public law. Effective e-governance requires a judiciary capable of addressing disputes arising from digital administration, including issues of electronic evidence, algorithmic decision-making, and data protection. However, where courts lack expertise in digital matters or adhere rigidly to traditional evidentiary standards, legal remedies may be inaccessible or ineffective (18). Comparative research indicates that judicial reluctance to engage with digital complexity can weaken oversight and embolden administrative non-compliance (19). Judicial barriers thus undermine the enforcement dimension of public law, reducing the practical significance of legal rights in the digital sphere.

Participatory–societal barriers complete the typology, drawing attention to the social conditions that shape citizens' engagement with digital governance. Legal recognition of participatory mechanisms does not automatically translate into meaningful involvement, particularly where digital divides, trust deficits, or cultural norms limit participation. Studies of open government initiatives demonstrate that participation often remains uneven, benefiting technologically savvy groups while excluding marginalized populations (20). From a public law perspective, such disparities raise concerns about equality and non-discrimination, as digital governance may inadvertently reinforce existing social inequalities. This typology underscores that barriers to e-governance are not isolated obstacles but interconnected constraints that span normative, institutional, judicial, and societal domains.

The Concept of "Digital Legal Failure"

The notion of "digital legal failure" provides a conceptual framework for understanding situations in which legal recognition of digital governance exists but fails to produce effective outcomes. Digital legal failure occurs when laws and policies formally endorse digital transformation, yet lack the operational capacity to shape administrative behavior. This phenomenon is not unique to any single jurisdiction; international studies have documented similar patterns where symbolic commitments to e-governance coexist with persistent implementation gaps (21). The concept emphasizes that legal existence alone is insufficient; what matters is the law's ability to structure incentives, allocate responsibilities, and enforce compliance.

Symbolic legislation plays a central role in digital legal failure. Such legislation often articulates ambitious goals, such as transparency, efficiency, or citizen participation, without specifying concrete obligations or sanctions. In the digital context, symbolic norms may authorize the creation of electronic platforms or promote interoperability without addressing governance questions related to data ownership, accountability, or oversight. Scholars have warned that symbolic digital reforms can create an illusion of progress while diverting attention from structural deficiencies (9). When digital governance is framed primarily as a technological upgrade rather than a legal transformation, enforcement mechanisms tend to be underdeveloped or absent.

The Iranian case exemplifies digital legal failure in several respects. Legal texts and policy documents frequently reference digital government objectives, yet these references are dispersed and lack binding force. This fragmentation allows administrative bodies to selectively adopt digital tools without altering underlying practices. Comparative analyses suggest that when digital governance lacks a coherent legal backbone, implementation becomes dependent on political will and administrative discretion rather than legal obligation (22). In Iran, this dynamic has resulted in uneven adoption, where some agencies pursue digital initiatives while others maintain traditional procedures, producing a hybrid system that undermines consistency and trust.

Digital legal failure also has implications for accountability. When digital systems malfunction or produce unjust outcomes, affected individuals may struggle to identify responsible actors or access effective remedies. Research on accountability in digital governance highlights the risk that responsibility becomes diffused across technological systems and organizational units, weakening traditional mechanisms of legal redress (11). In the absence of clear legal rules assigning responsibility, courts may be reluctant to intervene, reinforcing the gap between formal rights and practical enforcement. Digital legal failure thus reflects a broader tension between legal formalism and technological complexity, where existing legal categories prove inadequate to address new forms of governance.

Structural Incompatibility Between Traditional Administrative Law and Digital Governance

A critical source of e-governance barriers lies in the structural incompatibility between traditional administrative law and the logic of digital governance. Administrative law has historically been built around paper-based procedures, formal documentation, and hierarchical decision-making. Legality has been associated with written records, physical signatures, and sequential processes that ensure traceability and control. Digital governance, by contrast, relies on data-driven decision-making, real-time processing, and automated workflows that challenge these assumptions (17). This divergence creates friction when digital systems are introduced into legal environments designed for analog governance.

Formalism in administrative law, while serving important functions of predictability and control, can become a barrier when rigid adherence to traditional forms inhibits adaptation to digital processes. Requirements for physical documentation or in-person verification may persist even after electronic alternatives are introduced, resulting in parallel systems that increase complexity rather than efficiency. Studies of digital-era governance have shown that such hybrid arrangements often reflect institutional reluctance to relinquish familiar practices (2). In the Iranian context, formalistic legal culture reinforces this reluctance, as administrative legitimacy remains closely tied to traditional procedural symbols.

Hierarchy and secrecy further compound structural incompatibility. Traditional administrative systems prioritize centralized authority and control over information flows, whereas digital governance emphasizes openness, interoperability, and horizontal coordination. Research on network society dynamics suggests that digital technologies inherently disrupt hierarchical structures by enabling decentralized communication and data sharing (15). When legal frameworks continue to privilege secrecy and centralized control, digital initiatives may be constrained or distorted to fit existing power structures. This tension undermines the transformative potential of e-governance, reducing it to a technical overlay on unchanged institutional hierarchies.

Path dependency plays a crucial role in sustaining these incompatibilities. Administrative structures evolve incrementally, shaped by historical decisions that constrain future options. Once legal and institutional arrangements are established, they tend to persist even when their underlying rationale diminishes. Studies of institutional change highlight that reforms often encounter resistance not because alternatives are unavailable, but because existing arrangements are deeply embedded in organizational routines and legal doctrine (23). In Iran, the persistence of traditional administrative models reflects such path dependency, where digital governance initiatives must navigate a legal landscape designed for a different era.

The structural mismatch between traditional administrative law and digital governance thus represents a fundamental barrier that cannot be resolved through technological innovation alone. Without rethinking legal concepts of procedure, authority, and accountability, digital systems risk being assimilated into existing frameworks in ways that neutralize their transformative potential. Comparative experiences suggest that successful digital governance requires legal adaptation that aligns procedural norms with data-driven processes while preserving core public law values (7). Absent such adaptation, e-governance remains constrained by inherited legal forms, reinforcing the very inefficiencies and opacities it is intended to overcome.

Legislative and Normative Barriers to E-Governance in Iran

The legislative foundations of e-governance in Iran are marked by a fundamental structural deficiency: the absence of a comprehensive and unified e-governance law. Unlike jurisdictions that have consolidated digital governance principles within a single legislative framework, the Iranian legal system addresses digital administration through dispersed and sector-specific statutes. These statutes were often enacted for purposes unrelated to governance transformation and only incidentally touch upon electronic processes. Comparative scholarship on digital government has shown that such dispersion weakens the normative force of digital reform by depriving it of a clear legal identity and coherent objectives (6). When e-governance lacks a distinct statutory anchor, administrative bodies are left to interpret fragmented norms in isolation, producing uneven practices across the public sector.

This dispersion of legal norms has significant consequences for legal certainty and administrative accountability. Legal certainty requires that public authorities and citizens alike can ascertain applicable rules, responsibilities, and remedies with reasonable clarity. In the absence of a comprehensive e-governance law, digital obligations are scattered across unrelated legal texts, making it difficult to determine which rules govern specific digital interactions. Research on accountability frameworks emphasizes that clarity of legal mandates is a prerequisite for holding public actors responsible for their actions (11). In Iran, the lack of a unified legal framework allows administrative agencies to invoke ambiguity as a justification for non-compliance or selective implementation, thereby weakening accountability mechanisms. This ambiguity also complicates judicial review, as courts must navigate a fragmented normative landscape when assessing disputes arising from digital administration.

Regulatory ambiguity extends to the allocation of authority and responsibility within digital governance. Without a comprehensive statute defining institutional roles, it remains unclear which bodies are ultimately responsible for coordinating, supervising, or enforcing e-governance initiatives. Comparative studies have demonstrated that unclear allocation of authority leads to coordination failures and diffusion of responsibility, particularly in networked governance environments (17). In the Iranian context, this ambiguity enables administrative actors to deflect responsibility for digital failures onto other institutions, reinforcing a culture of non-accountability. The absence of a clear legal hierarchy among digital governance actors thus constitutes a core legislative barrier, one that undermines both effectiveness and trust.

Fragmentation and inconsistency among existing norms further exacerbate these challenges. The Iranian legal framework governing digital administration is characterized by overlapping competencies and competing mandates among different regulatory bodies. Various ministries, councils, and agencies claim authority over aspects of digital policy, data management, or electronic services, often based on loosely defined legal provisions. Public management research has shown that overlapping competencies create incentives for turf protection and inter-agency conflict, hindering coordinated action (8). In digital governance, where interoperability and coordination are essential, such fragmentation is particularly damaging. Instead of fostering integration, the legal framework institutionalizes fragmentation, embedding it within formal rules.

Conflicting regulatory mandates also emerge from inconsistencies between older statutes and newer digital initiatives. Traditional laws, drafted for paper-based administration, continue to impose procedural requirements that conflict with digital workflows. At the same time, newer regulations promoting electronic processes often lack the authority to override entrenched legal norms. Scholars have noted that digital governance reforms frequently stall when legacy legislation is not systematically updated to align with new practices (2). In Iran, this tension manifests in parallel systems where digital platforms coexist with mandatory paper procedures, generating inefficiencies and legal confusion. Administrative actors may comply with digital initiatives symbolically while relying on traditional processes to ensure legal defensibility, thereby neutralizing reform efforts.

The lack of a clear hierarchy among digital governance rules compounds these inconsistencies. In effective legal systems, higher-level norms provide guidance and coherence for lower-level regulations. However, in the Iranian digital governance landscape, policy documents, ministerial regulations, and statutory provisions often operate without a defined hierarchy. International analyses of digital government frameworks emphasize that hierarchical clarity is essential for resolving conflicts and ensuring consistent implementation (7). Without such clarity, administrative bodies may prioritize whichever norm aligns with their interests or capacities, resulting in selective compliance. This discretionary norm selection undermines the rule of law by allowing administrative convenience to override legal coherence.

Another critical legislative barrier lies in the weakness or absence of legal sanctions for non-compliance with digital governance obligations. Even where laws or policies encourage electronic processes, they rarely specify consequences for public bodies that fail to implement them. Accountability literature underscores that obligations without sanctions are unlikely to shape behavior, particularly in bureaucratic settings where compliance imposes costs or threatens established practices (12). In Iran, digital governance norms often function as aspirational guidelines rather than binding duties, signaling political commitment without creating enforceable obligations. This normative softness allows agencies to delay or disregard digital initiatives without fear of legal repercussions.

The prevalence of symbolic obligations further illustrates this problem. Symbolic legislation articulates values and goals without providing mechanisms for enforcement or evaluation. While such legislation may serve rhetorical or signaling purposes, it contributes to what scholars have described as “implementation gaps” in public administration (9). In the digital context, symbolic obligations may authorize the establishment of online platforms or data systems without mandating their use or integration into core administrative processes. As a result, e-governance becomes optional rather than mandatory, subject to administrative discretion and political priorities. This optionality undermines the transformative potential of digital governance, reducing it to a peripheral activity rather than a structural reform.

The absence of effective sanctions also has implications for equality and fairness. When compliance is discretionary, agencies with greater resources or political support may implement digital systems, while others lag behind, creating uneven access to digital services. Studies of digital government adoption highlight that uneven implementation exacerbates inequalities and undermines public trust (19). In Iran, such disparities reinforce perceptions that digital governance is inconsistent and unreliable, further discouraging citizen engagement. Legal sanctions, by contrast, could standardize expectations and ensure a minimum level of compliance across the public sector.

Budgetary and legislative neglect represents another significant normative barrier to e-governance. Digital transformation requires sustained financial investment in infrastructure, training, and maintenance. Yet, in the absence of binding fiscal commitments, digital initiatives are often treated as discretionary expenditures, vulnerable to budget cuts or shifting political priorities. Research on digital government emphasizes that stable funding is a critical determinant of success, as intermittent investment undermines system reliability and institutional learning (22). In Iran, digital projects frequently depend on short-term funding arrangements rather than long-term fiscal planning, reflecting their marginal status within legislative priorities.

The legal consequences of unfunded mandates are particularly problematic. When laws or policies require digital initiatives without allocating sufficient resources, they create obligations that cannot be fulfilled in practice. Public administration scholars have long warned that unfunded mandates erode institutional credibility and foster cynicism among implementers (8). In the digital governance context, unfunded mandates lead to partial or superficial implementation, as agencies attempt to comply symbolically without investing in necessary capacity. This dynamic reinforces the perception of e-governance as an optional add-on rather than a core administrative function.

Legislative neglect also manifests in the failure to integrate digital governance into budgetary oversight and accountability mechanisms. Without legal requirements to report on digital expenditures and outcomes, it is difficult to assess the effectiveness of investments or to hold agencies accountable for results. International frameworks stress the importance of linking digital governance to performance management and fiscal transparency (21). The absence of such linkages in Iran weakens legislative oversight and allows digital projects to operate outside rigorous evaluation, perpetuating inefficiencies and waste.

Normative resistance to transparency constitutes a deeper and more entrenched barrier within the Iranian legal system. Transparency is often celebrated as a central promise of e-governance, enabling citizens to access information and monitor public action. However, legal norms governing information disclosure in Iran reflect a secrecy-oriented administrative culture, where disclosure is treated as an exception rather than a default. Comparative research on transparency highlights that legal presumptions of secrecy undermine digital openness by legitimizing non-disclosure practices (20). In such contexts, digital platforms may exist, but the information they provide is limited or selectively curated.

Overbroad exceptions to information disclosure further entrench this resistance. Laws that allow public bodies to withhold information on vague grounds such as public interest or administrative convenience create wide discretion for non-disclosure. Accountability scholars argue that such exceptions weaken transparency by shifting the burden from the state to the citizen to justify access (11). In Iran, these exceptions are often embedded in legal texts without clear definitions or oversight mechanisms, enabling agencies to deny access to information even in digital contexts. This legal normalization of opacity contradicts the normative foundations of e-governance, which rely on openness to generate public value.

The normalization of opacity has broader implications for trust and participation. Digital governance initiatives that fail to deliver meaningful transparency may heighten public skepticism, as citizens encounter technologically sophisticated systems that reproduce traditional secrecy. Studies of network society dynamics suggest that digital tools can amplify both transparency and control, depending on the surrounding legal framework (15). When legal norms favor secrecy, digital systems may enhance administrative surveillance rather than public oversight, reinforcing power asymmetries. In Iran, this risk is exacerbated by the absence of strong legal safeguards for transparency and accountability in digital environments.

Taken together, these legislative and normative barriers reveal a pattern of partial and inconsistent legal adaptation to digital governance. The absence of a comprehensive e-governance law, combined with fragmented norms, weak sanctions, budgetary neglect, and entrenched secrecy, creates a legal environment in which digital transformation is rhetorically endorsed but structurally constrained. International experience suggests that overcoming such barriers requires not only technological investment but also deliberate legal reform that aligns digital initiatives with enforceable norms and institutional incentives (16). Without addressing these legislative foundations, e-governance in Iran remains vulnerable to symbolic adoption and practical dysfunction, perpetuating the gap between legal recognition and effective implementation.

Institutional, Judicial, and Participatory Barriers

Institutional and executive barriers constitute one of the most persistent obstacles to the realization of e-governance in Iran, as they directly affect the capacity of the state to translate legal norms and policy commitments into coordinated administrative action. A central feature of this problem is the lack of a clearly designated coordinating authority with comprehensive legal competence over e-governance. Digital governance inherently requires cross-sectoral coordination, as data flows, service platforms, and regulatory standards cut across traditional administrative boundaries. Comparative research on interoperability in e-government demonstrates that without a central coordinating body empowered to set binding standards and resolve conflicts, digital initiatives tend to fragment along institutional lines (17). In Iran, multiple agencies claim partial authority over digital policies, information systems, or administrative modernization, yet none possesses unequivocal leadership backed by a comprehensive legal mandate. This multiplicity of actors produces policy incoherence, as agencies pursue divergent priorities and timelines, often resulting in overlapping platforms or incompatible systems.

The absence of clear leadership also contributes to implementation paralysis. When no single institution bears ultimate responsibility for e-governance outcomes, failures can be attributed to coordination problems rather than substantive deficiencies. Public management literature emphasizes that diffusion of responsibility is a common feature of governance failure in complex administrative systems (9). In the Iranian context, this diffusion allows executive bodies to defer action, citing the need for inter-agency consensus or higher-level authorization. As a result, digital initiatives may be announced repeatedly without reaching operational maturity, reinforcing perceptions of stagnation. International assessments of digital government highlight that effective coordination mechanisms are critical for overcoming such paralysis, particularly in centralized administrative systems (7).

Bureaucratic resistance and organizational inertia further compound institutional barriers. Digital governance often threatens established administrative routines by introducing transparency, automation, and data-driven oversight. For administrative elites accustomed to discretionary authority, these changes can be perceived as risks to professional autonomy and institutional influence. Research on street-level bureaucracy illustrates how officials may resist reforms that constrain discretion or expose decision-making to scrutiny (13). In digital contexts, transparency enabled by online platforms and integrated databases challenges informal practices and power asymmetries, prompting resistance that may manifest as passive non-compliance, selective implementation, or technical obstruction.

This resistance is reinforced by organizational inertia rooted in longstanding administrative cultures. Digital governance requires not only new technologies but also changes in organizational norms, skills, and incentives. Studies of digital-era governance have shown that organizations often adapt new technologies to existing practices rather than transforming those practices, resulting in superficial change (2). In Iran, this pattern is evident in the persistence of parallel paper-based procedures alongside digital platforms, reflecting reluctance to abandon familiar modes of operation. Such inertia undermines the efficiency gains promised by e-governance and perpetuates skepticism among citizens who encounter redundant or inconsistent processes.

Regulatory fragmentation at the executive level represents another significant barrier. In the absence of a unified legislative framework, executive authorities often resort to issuing by-laws, circulars, and internal directives to regulate digital initiatives. While these instruments can provide short-term guidance, their proliferation creates normative overload without integration. Scholars have warned that excessive reliance on subordinate regulations can obscure legal obligations and weaken compliance, particularly when such instruments lack transparency or consistency (8). In Iran, the accumulation of executive directives related to digital administration has produced a dense but disjointed regulatory environment, where officials struggle to reconcile competing instructions.

Normative overload also complicates accountability. When obligations are dispersed across numerous circulars and guidelines, it becomes difficult to determine which norms are binding and which are merely advisory. Accountability frameworks emphasize that clarity and hierarchy of norms are essential for effective oversight (11). Without such clarity, executive bodies may prioritize convenience or political considerations over legal consistency, reinforcing discretionary governance. This fragmentation at the executive level thus mirrors legislative dispersion, creating a multi-layered barrier that constrains e-governance implementation.

Judicial barriers play a crucial role in shaping the effectiveness of e-governance, as courts are responsible for interpreting digital norms and providing remedies when rights are violated. One of the most pressing challenges in this domain is the absence of a well-developed doctrine of digital evidence. Traditional evidentiary rules in many legal systems were designed for physical documents and in-person transactions, emphasizing tangible records and formal authentication. In digital governance, however, interactions increasingly occur through electronic records, automated logs, and data trails. Comparative studies indicate that courts often struggle to adapt evidentiary standards to these new forms, leading to uncertainty and inconsistency (18). In Iran, reliance on traditional proof mechanisms creates insecurity regarding the legal status of electronic records, discouraging both administrators and citizens from fully trusting digital processes.

This insecurity has practical consequences for litigation involving digital administration. When electronic records are treated as secondary or unreliable evidence, litigants may face difficulties in proving claims related to digital services or automated decisions. Research on digital government underscores that legal certainty regarding electronic evidence is essential for fostering trust and compliance (19). In the absence of clear judicial doctrine, administrative bodies may revert to paper-based documentation to ensure legal defensibility, undermining the efficiency and transparency of digital systems. This dynamic illustrates how judicial conservatism can indirectly reinforce institutional resistance to e-governance.

Weak judicial interpretation of digital rights further exacerbates these challenges. Courts play a pivotal role in translating abstract legal principles into concrete protections, particularly in emerging areas such as data protection, algorithmic decision-making, and online participation. However, when judges adopt a strictly formalist reading of laws, they may fail to account for the unique risks and opportunities associated with digital governance. Accountability scholars argue that purposive interpretation is necessary to adapt legal principles to new contexts, ensuring that rights remain effective (12). In Iran, the limited development of digital jurisprudence reflects a cautious approach that prioritizes textual fidelity over normative adaptation.

The failure to develop a purposive digital jurisprudence has broader implications for governance. Without judicial recognition of digital rights as substantive extensions of existing constitutional and administrative principles, legal protections remain fragmented and reactive. Comparative analyses suggest that proactive judicial engagement is critical for shaping norms around transparency, privacy, and participation in digital governance (1). In the Iranian context, judicial restraint leaves these issues largely unaddressed, allowing executive practices to evolve without robust legal scrutiny.

The lack of specialized courts or judges with expertise in digital governance constitutes another judicial barrier. Digital administration involves complex technical issues, including data architectures, cybersecurity, and algorithmic processes, which may exceed the familiarity of generalist judges. Research on judicial capacity indicates that specialization enhances consistency and quality of adjudication in technically complex areas (14). In Iran, the absence of institutionalized specialization means that digital disputes are often adjudicated by judges without targeted training, increasing the likelihood of inconsistent rulings and procedural delays.

These capacity constraints undermine legal predictability, a core element of the rule of law. When parties cannot anticipate how courts will assess digital evidence or interpret digital rights, they may hesitate to rely on electronic systems. Studies of digital government adoption highlight that predictability in legal outcomes is a key determinant of trust and participation (22). Judicial uncertainty thus feeds back into institutional reluctance, reinforcing a cycle in which digital governance remains underutilized.

Ineffective judicial oversight of state digital platforms represents a further barrier with significant implications for accountability. Digital platforms operated by public authorities collect, process, and store vast amounts of personal data, raising concerns about privacy and misuse. Effective oversight requires courts to scrutinize platform design, data practices, and decision-making processes. However, when judicial review is limited to formal legality rather than substantive assessment, oversight remains superficial. Comparative research on open government initiatives suggests that weak oversight enables administrative opacity and erodes public trust (20). In Iran, limited judicial engagement with privacy violations and data governance issues allows systemic problems to persist without correction.

The absence of systemic accountability mechanisms exacerbates this problem. Without coordinated oversight that addresses structural issues rather than isolated cases, judicial intervention remains fragmented. Accountability frameworks emphasize the importance of systemic review in complex governance environments, where individual cases may not reveal broader patterns of dysfunction (11). The lack of such review in Iran's digital governance landscape limits the judiciary's capacity to function as an effective check on executive power.

Participatory and societal barriers complete the picture of e-governance constraints by highlighting how digital governance shapes, and is shaped by, citizen engagement. A central issue in this domain is the prevalence of state-centric digital design, where platforms are structured primarily to serve administrative needs rather than to empower citizens as rights holders. Digital governance systems often conceptualize citizens as data subjects whose information is collected and processed, rather than as active participants in decision-making. International studies have noted that such designs reinforce one-way information flows, limiting opportunities for meaningful interaction (16). In Iran, state-centric design reflects broader administrative traditions that prioritize control and efficiency over participatory governance.

This orientation has normative implications for public law. Participation is not merely a technical feature but a legal principle tied to democratic legitimacy. When digital platforms facilitate information dissemination without providing channels for feedback or contestation, they fall short of participatory ideals. Research on digital government underscores that participation requires institutionalized procedures that ensure citizen input influences outcomes (24). The absence of such procedures in Iranian digital platforms contributes to disengagement and skepticism, undermining the democratic potential of e-governance.

Digital inequality and access gaps further constrain participation. Effective e-governance presupposes that citizens possess the necessary infrastructure, skills, and resources to engage with digital platforms. However, geographic disparities, economic constraints, and educational differences can limit access, creating structural exclusion. Comparative analyses highlight that digital divides persist even in technologically advanced societies, necessitating targeted legal and policy interventions (21). In Iran, such disparities are exacerbated by uneven infrastructure development and limited digital literacy programs, restricting participation to relatively privileged groups.

These access gaps have legal significance, as they implicate principles of equality and non-discrimination. When digital governance becomes a primary mode of service delivery, those excluded from digital access may face indirect discrimination. Studies of digital governance stress that inclusive design and alternative access mechanisms are essential to uphold legal equality (19). The absence of such safeguards in Iran reinforces societal barriers, limiting the reach and legitimacy of e-governance initiatives.

Trust deficit and privacy anxiety represent deeper societal barriers that influence citizen engagement. Digital governance involves extensive data collection, raising concerns about surveillance and misuse. In contexts where legal protections for privacy are perceived as weak, citizens may fear that participation exposes them to monitoring or retaliation. Research on network societies indicates that digital technologies can amplify surveillance capacities, intensifying trust concerns (15). In Iran, such concerns contribute to a chilling effect on participation, as citizens refrain from engaging with digital platforms to avoid potential risks.

Privacy anxiety also undermines the credibility of digital governance initiatives. When citizens doubt that their data will be protected or used responsibly, they may question the legitimacy of digital systems. Accountability literature highlights that trust is a precondition for effective governance, particularly in digital contexts where interactions are mediated by technology rather than personal contact (1). Without robust legal assurances and visible enforcement, trust deficits persist, reinforcing participatory barriers.

Taken together, institutional, judicial, and participatory barriers form an interconnected web that constrains e-governance in Iran. Institutional fragmentation and resistance limit coordinated action, judicial constraints weaken enforcement and oversight, and societal barriers restrict meaningful participation. International experience suggests that addressing these barriers requires integrated reform across legal, institutional, and social domains (7). In the absence of such integration, e-governance remains a partial and contested project, constrained by structural factors that extend beyond technology and into the core of public law and governance.

Conclusion

This study set out to explain why e-governance has failed to achieve effective and coherent implementation in Iran despite repeated legal recognition, policy emphasis, and technological investment. Rather than approaching the issue through the familiar language of prerequisites and ideal conditions, the analysis deliberately focused on barriers—those structural, legal, institutional, judicial, and societal forces that actively obstruct the translation of digital ambitions into operational governance. The findings demonstrate that the shortcomings of e-governance in Iran are not primarily technical, nor can they be attributed to a lack of policy awareness. Instead, they are rooted in deeper problems of legal design, institutional organization, judicial capacity, and participatory legitimacy.

At the legislative and normative level, the absence of a comprehensive e-governance law has produced a fragmented legal landscape in which digital governance lacks a clear identity and binding force. Digital norms are dispersed across unrelated statutes, policy documents, and executive regulations, resulting in ambiguity about authority, responsibility, and enforceability. This dispersion undermines legal certainty and allows administrative bodies to treat e-governance as discretionary rather than mandatory. Without clear sanctions for non-compliance and without binding fiscal commitments, digital initiatives remain vulnerable to delay, dilution, or symbolic adoption. The normalization of opacity within the legal system, reinforced by overbroad exceptions to transparency, further weakens the transformative promise of digital governance by embedding secrecy into the normative framework itself.

Institutional and executive barriers amplify these legislative weaknesses. The lack of a central coordinating authority with a clear legal mandate has led to policy incoherence and implementation paralysis. Multiple agencies operate in parallel, often pursuing incompatible digital strategies while avoiding responsibility for collective outcomes. Bureaucratic resistance and organizational inertia, fueled by perceived threats to discretionary power and professional autonomy, further obstruct meaningful reform. Rather than transforming administrative practices, digital tools are frequently assimilated into existing routines, producing parallel systems that preserve traditional hierarchies and procedural formalism. Regulatory fragmentation at the executive level compounds these problems, as the proliferation of by-laws and circulars creates normative overload without integration or clarity.

Judicial barriers represent a critical but often overlooked dimension of e-governance failure. Courts play a central role in giving practical meaning to legal norms, yet the absence of a developed doctrine of digital evidence, combined with reliance on traditional proof mechanisms, undermines confidence in electronic records and automated processes. Weak judicial interpretation of digital rights, rooted in formalistic readings of law, has prevented the emergence of a purposive digital jurisprudence capable of addressing the realities of data-driven governance. The lack of specialized courts or judges with expertise in digital matters further erodes legal predictability, discouraging both citizens and administrators from relying on digital systems. Ineffective judicial oversight of state digital platforms, particularly in relation to privacy and data governance, leaves systemic problems unaddressed and allows accountability gaps to persist.

Participatory and societal barriers reveal how digital governance interacts with broader patterns of power, trust, and inequality. State-centric digital design has positioned citizens primarily as data subjects rather than as rights holders or active participants in governance. One-way information flows dominate, while meaningful channels for feedback, contestation, and co-decision remain underdeveloped. Digital inequality, shaped by geographic, economic, and educational disparities, excludes significant segments of society from effective participation, raising concerns about equality and non-discrimination. Trust deficits and privacy anxiety further discourage engagement, as citizens fear surveillance, data misuse, or adverse consequences of participation. In such an environment, digital governance risks reinforcing existing power asymmetries rather than democratizing public authority.

Taken together, these findings point to a central conclusion: e-governance in Iran has been treated primarily as a technological and managerial project, while its legal and institutional foundations have remained underdeveloped. This imbalance has produced a form of digital governance that is formally recognized but substantively weak, symbolically ambitious but operationally fragile. The result is a persistent gap between legal acknowledgment and practical implementation, a gap sustained by structural barriers rather than by isolated policy failures.

The analysis also highlights a broader theoretical implication. Digital transformation does not automatically modernize governance; when introduced into legal and institutional environments shaped by formalism, hierarchy, and secrecy, digital tools may be absorbed in ways that reproduce existing dysfunctions. Without enforceable legal norms, clear institutional responsibility, effective judicial oversight, and inclusive participatory mechanisms, digital governance can become a façade—visible in platforms and portals, yet absent in accountability, transparency, and public trust. In such circumstances, digitalization may even intensify control and opacity rather than limiting them.

This study does not claim that the barriers identified are unique to Iran, nor does it suggest that digital governance failure is inevitable. Instead, it shows that e-governance is a deeply legal and institutional phenomenon, one that succeeds or fails depending on how public power is structured, constrained, and legitimized in the digital age. By foregrounding barriers rather than ideals, the analysis offers a more realistic and critical understanding of why reform efforts have stalled and why technological investment alone has proven insufficient.

Ultimately, the future of e-governance in Iran depends on whether digital transformation is accompanied by a corresponding transformation of public law and governance institutions. Without addressing legislative fragmentation, institutional incoherence, judicial incapacity, and participatory exclusion, digital initiatives will continue to operate at the margins of governance rather than at its core. The lesson that emerges from this study is clear: e-governance cannot be built on technology alone. It must be grounded in enforceable law, coherent institutions, accountable courts, and an empowered citizenry. Only then can digital governance move beyond symbolism and become a meaningful mode of exercising public authority.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Bannister F, Connolly R. ICT, public values and transformative government: A framework and programme for research. Government Information Quarterly. 2014;31(1):119-28.
2. Dunleavy P, Margetts H, Bastow S, Tinkler J. Digital era governance: IT corporations, the state, and e-government. Oxford: Oxford University Press; 2006.
3. Margetts H, Dunleavy P. The second wave of digital-era governance. Philosophical Transactions of the Royal Society A. 2013;371(1987).
4. Brown I, Marsden C. Regulating code: Good governance and better regulation in the information age. Cambridge, MA: MIT Press; 2013.
5. Lessig L. Code: Version 2.0. New York: Basic Books; 2006.
6. Gil-García JR. Enacting electronic government success: An integrative study of government-wide websites. New York: Springer; 2012.
7. Oecd. The OECD digital government policy framework. Paris: OECD Publishing; 2020.
8. Pollitt C, Bouckaert G. Public management reform: A comparative analysis. Oxford: Oxford University Press; 2017.
9. Kettl DF. The transformation of governance: Public administration for twenty-first century America. Baltimore: Johns Hopkins University Press; 2015.

10. Janssen M, Charalabidis Y, Zuiderwijk A. Benefits, adoption barriers and myths of open data and open government. Information Systems Management. 2012;29(4):258-68.

11. Bovens M, Goodin RE, Schillemans T. The Oxford handbook of public accountability. Oxford: Oxford University Press; 2014.

12. Hood C. Accountability and transparency: Siamese twins, matching parts, awkward couple? West European Politics. 2010;33(5):989-1009.

13. Lipsky M. Street-level bureaucracy: Dilemmas of the individual in public services. New York: Russell Sage Foundation; 2010.

14. Gil-García JR, Dawes SS, Pardo TA. Digital government and public management research: Finding the crossroads. Public Management Review. 2018;20(5):633-46.

15. Castells M. The rise of the network society. Oxford: Wiley-Blackwell; 2010.

16. United N. E-Government Survey 2022: The future of digital government. New York: United Nations Department of Economic and Social Affairs, 2022.

17. Janssen M, Estevez E, Janowski T. Interoperability in e-government. Government Information Quarterly. 2014;31(1):1-5.

18. Misuraca G, Pasi G, Viscusi G. AI and public sector decision-making: Legal and ethical challenges. European Journal of ePractice. 2020;12(1).

19. Zuiderwijk A, Chen Y-C, Salem F. Implications of digital government research for governance theory and practice. Information Polity. 2021;26(1):1-16.

20. Peled A. When transparency and collaboration collide: The USA Open Government initiative. Journal of the American Society for Information Science and Technology. 2011;62(11):2085-94.

21. Oecd. Digital government in the era of digital transformation. Paris: OECD Publishing; 2021.

22. West DM. Digital government: Technology and public sector performance. Princeton: Princeton University Press; 2005.

23. Fountain JE. Building the virtual state: Information technology and institutional change. Washington, DC: Brookings Institution Press; 2001.

24. Cordella A, Bonina CM. A public value perspective for ICT enabled public sector reforms: A theoretical reflection. Government Information Quarterly. 2012;29(4):512-20.