

Challenges of E-Government in Enhancing the Efficiency of Public Administration and Safeguarding Citizens' Public Rights: A Comparative Study of Iran and the United Kingdom

Mehrdad. Jamal Arvanaghi¹, Ahmad. Ranjbar^{1*}, Alireza. Saybani², Mohammad. Bahadori Jahromi³

¹ Department of Law, B.A.C., Islamic Azad University, Bandar Abbas, Iran

² Department of Criminal Law and Criminology, B.A.C., Islamic Azad University, Bandar Abbas, Iran

³ Department of Law, Tarbiat Modares University, Tehran, Iran

* Corresponding author email address: ranjbar.ahd@iau.ac.ir

Received: 2026-02-10

Revised: 2026-07-21

Accepted: 2026-07-28

Initial Publish: 2026-07-28

Final Publish: 2026-11-01

The digital transformation of public administration has altered the delivery of public services, the exercise of administrative authority, and the relationship between governments and citizens. Although e-government can reduce bureaucratic procedures, accelerate service delivery, improve institutional coordination, and facilitate access to administrative information, it may also generate legal, institutional, managerial, and technological risks that undermine both administrative efficiency and citizens' public rights. This article comparatively examines these challenges in Iran and the United Kingdom through a qualitative, descriptive-analytical, and comparative legal method. The analysis focuses on institutional fragmentation, weak interoperability, digital reproduction of traditional bureaucracy, unequal organisational capacity, cybersecurity threats, infrastructure failure, poor data quality, digital exclusion, privacy risks, concentration of governmental information, algorithmic discrimination, limited transparency, unclear administrative responsibility, inadequate human assistance, and barriers to effective complaint and remedy. The findings indicate that Iran's principal difficulties arise from fragmented digital systems, uneven institutional capacity, incomplete data-governance safeguards, insufficient interoperability, and uncertainty regarding responsibility for digital administrative errors. The United Kingdom benefits from comparatively stronger coordination, service-design standards, data-protection mechanisms, accessibility requirements, and administrative-review structures; nevertheless, it continues to face serious concerns relating to digital exclusion, automated welfare administration, outsourcing, algorithmic opacity, cybersecurity, and the concentration of informational power. The article argues that e-government does not automatically produce efficient or rights-compatible administration. Its legitimacy and effectiveness depend on the establishment of a rights-based digital-governance framework grounded in legality, equality, accessibility, transparency, accountability, privacy, data security, proportionality, human review, and effective remedies. The study concludes that administrative efficiency and the protection of citizens' rights should be treated as mutually reinforcing objectives. Sustainable digital-government reform therefore requires coordinated legal regulation, institutional integration, administrative-process redesign, inclusive service delivery, resilient infrastructure, and enforceable mechanisms for reviewing and correcting digital administrative decisions.

Keywords: E-Government; Digital Governance; Public Administration; Administrative Efficiency; Citizens' Public Rights; Administrative Law; Digital Transformation; Data Protection; Algorithmic Decision-Making; Iran; United Kingdom

How to cite this article:

Jamal Arvanaghi, M., Ranjbar, A., Saybani, A., & Bahadori Jahromi, M. (2026). Challenges of E-Government in Enhancing the Efficiency of Public Administration and Safeguarding Citizens' Public Rights: A Comparative Study of Iran and the United Kingdom. *Interdisciplinary Studies in Society, Law, and Politics*, 5(6), 1-20. <https://doi.org/10.61838/kman.isslp.523>



1. Introduction

The expansion of information and communication technologies has fundamentally altered the organisation of public authority, the delivery of administrative services, and the relationship between governments and citizens. Public institutions increasingly rely on electronic portals, interconnected databases, digital identification systems, automated procedures, and data-driven decision-making to carry out functions that were traditionally performed through paper-based processes and direct interactions between officials and members of the public. E-government initially emerged as a mechanism for transferring administrative information and services to electronic environments, but its contemporary meaning extends far beyond the establishment of websites or the digital submission of forms. It now encompasses the redesign of administrative procedures, integration of governmental databases, electronic participation, digital communication between public bodies and citizens, and, increasingly, the use of automated systems in allocating benefits, determining eligibility, identifying risks, and exercising regulatory authority. Shakeri describes e-government as a systematic transformation in how governmental functions and public services are organised through technology rather than merely an additional channel for administrative communication (Shakeri, 2011). This transformation has created significant expectations regarding the reduction of bureaucracy, acceleration of public services, improvement of institutional coordination, and strengthening of governmental responsiveness. At the same time, it has generated new legal and institutional questions concerning the concentration of information, privacy, equal access, administrative transparency, responsibility for technological errors, and the ability of citizens to challenge digitally mediated governmental decisions.

The importance of e-government is particularly evident when it is examined through the concept of public-administration efficiency. Traditional public administration has frequently been criticised for excessive procedural formalism, institutional fragmentation, slow decision-making, repetitive documentary requirements, and high administrative costs. Digitalisation promises to reduce these

deficiencies by allowing information to be processed more rapidly, enabling public bodies to share data, facilitating remote access to administrative services, and reducing unnecessary physical contact between citizens and officials. Alvani explains that administrative efficiency cannot be reduced to the mechanical reduction of costs because it also includes the capacity of public institutions to achieve public objectives, respond to social needs, coordinate organisational resources, and maintain the quality of public services (Alvani, 2016). This broader conception is particularly important in the digital context. A service cannot be regarded as genuinely efficient merely because it is delivered quickly if it is inaccessible to vulnerable citizens, founded on inaccurate data, incapable of handling exceptional circumstances, or structured in a way that prevents meaningful review. Administrative efficiency must therefore be evaluated in relation to legality, service quality, accessibility, institutional reliability, and the capacity to correct errors. The transition from conventional administration to digital administration does not eliminate these requirements; rather, it changes the conditions under which they must be realised.

From the perspective of public law, the digitalisation of administration is not a politically or legally neutral process. Public administration is the institutional mechanism through which governmental authority is exercised and public rights are recognised, limited, implemented, or denied. Administrative procedures determine whether individuals receive licences, social support, education, healthcare, taxation decisions, regulatory approvals, and many other benefits or burdens arising from the exercise of public power. Tabatabaei Motameni observes that administrative law is fundamentally concerned with regulating the organisation, competence, procedures, and accountability of administrative authorities in their relations with individuals (Tabatabaei Motameni, 2020). When those relations are transferred to digital systems, the traditional principles of administrative law remain applicable, but the manner in which they operate becomes more complex. The legal basis of an administrative act may be difficult to identify when a decision is produced through interconnected systems. Responsibility may become dispersed among a public authority, a software developer, a database administrator, and a private contractor. The reasons for

a decision may be hidden within technical rules that neither the citizen nor the responsible public official fully understands. The transition to e-government therefore transforms not only the instruments of administration but also the practical environment in which legality, equality, accountability, and administrative justice must be guaranteed.

This transformation creates a central tension between the operational objectives of digital government and the normative obligations of public administration. Governments may pursue digitalisation to increase speed, reduce expenditure, standardise decisions, and improve control over administrative processes. Citizens, however, are entitled to expect that those objectives will not be achieved at the expense of privacy, procedural fairness, equal access, or the right to contest governmental decisions. Gorji Azandariani emphasises that public law subjects governmental power to principles that protect the public interest and prevent arbitrary exercises of authority ([Gorji Azandariani, 2016](#)). In a digital environment, these principles require more than the formal existence of legal rules. They require technological systems to be designed and operated in a manner compatible with the rule of law. A system that automatically excludes an eligible applicant because of inaccurate information, a portal that is inaccessible to persons with disabilities, or an automated process that provides no intelligible reasons may operate with technical consistency while remaining legally defective. The central challenge is consequently not whether governments should use technology, but how digital administrative power should be organised so that technological efficiency remains subordinate to lawful public purposes and effective protection of citizens.

The comparative study of Iran and the United Kingdom is valuable because the two systems display different levels of digital maturity, administrative coordination, regulatory development, and institutional capacity, while both confront common problems created by the increasing dependence of public administration on technology. Iran has made substantial efforts to expand electronic public services, create national administrative portals, connect governmental databases, and reduce the need for physical attendance at public offices. These initiatives have produced important gains in accessibility and administrative speed, but their effectiveness is

limited by fragmented systems, unequal digital capacity among public institutions, incomplete legal regulation of personal data, inconsistent interoperability, and difficulties in identifying responsibility for electronic errors. The United Kingdom represents a more institutionally developed model of digital public administration, characterised by comparatively established service standards, stronger traditions of administrative review, greater emphasis on user-centred design, and more developed mechanisms of data protection and public accountability. Nevertheless, digitalisation in the United Kingdom has also created serious concerns regarding digital exclusion, automated welfare administration, outsourcing, algorithmic opacity, and the growing informational power of the state. Ranchordas demonstrates that digital welfare systems can convert legal rights into technically conditional forms of access, in which the ability to receive public support increasingly depends on navigating digital procedures and satisfying automated classifications ([Ranchordas, 2023](#)). The comparative value of the English experience therefore lies not in presenting it as a flawless model but in examining both its institutional strengths and its continuing rights-related vulnerabilities.

The conceptual movement from e-government to digital transformation further increases the significance of this comparison. Mergel and her colleagues distinguish digital transformation from the simple adoption of technological instruments by emphasising its effects on organisational structures, administrative culture, service design, and institutional relationships ([Mergel et al., 2019](#)). A government may introduce electronic forms without reforming the procedures that make those forms complicated, or establish an integrated portal while preserving the fragmented responsibilities of the institutions behind it. In such circumstances, digitalisation may reproduce bureaucracy in electronic form rather than eliminate it. The distinction between technological adoption and institutional transformation is therefore central to the present analysis. Iran's experience illustrates the limitations of digital development when technical projects are not consistently accompanied by legal harmonisation and administrative-process reform. The United Kingdom illustrates how common standards and central coordination may improve service delivery while still

leaving unresolved questions concerning transparency, exclusion, and automated decision-making. The comparison thus enables the article to identify the conditions under which digitalisation becomes a means of substantive administrative reform rather than a superficial change in the appearance of bureaucracy.

The principal objective of this article is to analyse the legal, institutional, managerial, and technological challenges that limit the capacity of e-government to enhance the efficiency of public administration while safeguarding citizens' public rights in Iran and the United Kingdom. It seeks to determine how administrative efficiency should be understood in a digital environment, which public rights are most vulnerable to digital transformation, why similar technologies may produce different effects in different administrative systems, and which elements of the English experience may be adapted to the Iranian legal and institutional context. The article adopts a descriptive-analytical and comparative legal method. It does not attempt to measure the number of digital services or rank the technological performance of the two countries. Instead, it examines the normative quality of digital administration by assessing whether electronic systems support legality, equality, transparency, accessibility, administrative justice, data security, accountability, and effective remedies.

The argument advanced here is that e-government does not automatically create efficient administration or stronger protection of citizens' rights. Its consequences depend on the legal and institutional framework governing the use of technology. Bannister and Connolly caution that digital-government initiatives must be assessed in relation to public values rather than solely according to economic or technological indicators (Bannister & Connolly, 2014). This insight is especially important because some apparent efficiency gains may conceal transfers of administrative burdens from the government to citizens. An online procedure may reduce the workload of an administrative office while requiring applicants to obtain digital equipment, upload complex documents, resolve system errors, and repeatedly verify information already held by other public bodies. Similarly, automation may produce faster decisions while reducing the opportunity for officials to recognise exceptional circumstances. A legally sound evaluation of e-government must therefore consider who benefits

from digitalisation, who bears its costs, which groups face exclusion, and whether the resulting system preserves meaningful human and legal accountability.

The article develops the concept of rights-based digital governance as an analytical framework for addressing these questions. Under this framework, technology is neither treated as an autonomous solution nor rejected as an inherent threat to rights. It is understood as an instrument of public authority that must be governed by public-law principles. Administrative efficiency and the safeguarding of public rights are accordingly regarded as complementary elements of legitimate digital government. Efficiency without rights may produce fast but arbitrary administration, while rights without adequate administrative capacity may remain formally recognised but practically inaccessible. The following sections first clarify the conceptual and normative foundations of rights-based e-government, then examine the legal and institutional contexts of Iran and the United Kingdom, and subsequently provide a comparative analysis of the major challenges affecting administrative efficiency and public rights. The conclusion identifies the conditions necessary for moving from a predominantly technological conception of e-government toward an integrated model of lawful, inclusive, accountable, and resilient digital governance.

2. Conceptual and Normative Framework of Rights-Based E-Government

A clear conceptual distinction must initially be drawn between digitisation, e-government, digital transformation, and digital governance. Digitisation refers to the conversion of information, records, and documents from physical to electronic formats. It may improve storage, retrieval, and communication without substantially altering the underlying administrative process. E-government is broader and involves the use of electronic technologies in the delivery of services, internal administration, inter-agency communication, and interaction between government and citizens. Shakeri explains that e-government includes multiple forms of interaction, including government-to-citizen, government-to-business, government-to-government, and government-to-employee relations (Shakeri, 2011). Digital transformation goes further by requiring the redesign of institutional processes, organisational structures, public-service models, and administrative

culture. Mergel's analysis demonstrates that genuine digital transformation involves organisational change and the reconfiguration of public-sector practices rather than the mere introduction of technological tools (Mergel et al., 2019). Digital governance is the most comprehensive concept because it concerns how technology influences the exercise of authority, the formulation of policy, the distribution of responsibilities, the management of public data, and the participation of citizens in governmental processes.

These distinctions are legally significant because the risks associated with each stage are different. The digitisation of records raises questions concerning data accuracy, security, and access. Electronic service delivery raises issues of accessibility, identity verification, procedural design, and continuity. Integrated digital administration creates concerns about inter-agency data sharing, institutional responsibility, and the concentration of information. Automated administration introduces questions concerning explainability, discrimination, human review, and the legal status of algorithmically generated decisions. Wirtz and his colleagues show that artificial intelligence in the public sector may support forecasting, classification, resource allocation, and administrative decision-making, but its use also creates challenges relating to transparency, data quality, accountability, and ethical legitimacy (Wirtz et al., 2019). A rights-based analysis must therefore recognise that e-government is not a single uniform phenomenon. The legal safeguards required for a public-information website are not sufficient for a system that automatically determines eligibility for a public benefit or identifies individuals for regulatory investigation.

The concept of administrative efficiency similarly requires careful definition. In private-sector management, efficiency is often understood as the maximisation of output with minimum expenditure. Public administration operates under different normative conditions because governmental institutions are not merely service providers; they exercise legal authority and are responsible for advancing public interests. Alvani argues that effective public management requires the coordination of resources, organisational capacities, and public objectives rather than a narrow concern with financial savings (Alvani, 2016). Administrative efficiency in a digital context

should therefore include the speed of service delivery, reduction of unnecessary procedures, accuracy of decisions, accessibility of services, coordination between public bodies, continuity during crises, responsiveness to individual circumstances, and capacity to identify and correct errors. A system that processes applications rapidly but repeatedly makes incorrect decisions cannot be regarded as efficient. Nor can a platform be considered efficient when it reduces governmental expenditure by shifting administrative complexity onto citizens.

The distinction between efficiency and effectiveness is particularly relevant. Efficiency concerns the relationship between resources and outputs, whereas effectiveness concerns the extent to which public objectives are achieved. Digital systems may be efficient in processing large numbers of transactions but ineffective in ensuring that citizens actually receive the services to which they are entitled. For instance, a highly standardised online process may handle ordinary applications quickly but fail when a citizen's circumstances do not correspond to predetermined categories. The resulting system may appear successful according to quantitative indicators while producing significant substantive injustice. Doan's analysis of digital transformation in civil administrative services demonstrates that technological reform must be evaluated in relation to governance capacity, service accessibility, institutional coordination, and social development rather than by technological deployment alone (Doan, 2025). This approach supports a multidimensional understanding of efficiency in which administrative performance and citizens' practical ability to exercise their rights are assessed together.

Public-law principles establish the normative limits within which digital efficiency must operate. Administrative authorities possess powers that are legally conferred for specific public purposes. Tabatabaei Motameni notes that administrative competence is not a general freedom to act but a legally defined authority constrained by statutory objectives and procedural requirements (Tabatabaei Motameni, 2020). Digital systems cannot expand administrative competence beyond those limits. If an authority is not legally entitled to collect or share particular information, the technical capacity to do so does not create a lawful basis. Similarly, automation cannot transform a discretionary power into

an inflexible rule when legislation requires individual assessment. Xu's account of law-based administrative governance emphasises that technological and economic change does not displace the requirement that administrative power remain grounded in law, exercised proportionately, and subject to oversight (Xu, 2024). Rights-based e-government consequently requires legality to be embedded in technological design, data architecture, institutional arrangements, and decision-making procedures.

The rule of law in digital administration has both formal and substantive dimensions. Formally, public authorities must possess a clear legal basis for collecting data, integrating databases, using automated tools, and issuing electronic decisions. Citizens must be able to identify the institution responsible for an action and the rule under which it was taken. Substantively, the system must be predictable, non-arbitrary, and compatible with recognised rights. Abbasi explains that contemporary administrative law is concerned not only with controlling institutional competence but also with ensuring fairness, proportionality, transparency, and protection against abuse of public power (Abbasi, 2025). These principles acquire new importance when administrative actions are generated through technological systems. A citizen may not know whether an adverse decision resulted from a legal rule, an administrative policy, an incorrect database entry, a software configuration, or an automated risk score. Unless the system can reveal the relevant decision-making pathway, legality becomes difficult to assess and judicial or administrative review loses effectiveness.

Equality is another essential component of rights-based digital governance. Digital services may expand access by eliminating geographical distance, reducing travel costs, and allowing citizens to interact with public institutions outside conventional working hours. Yet digitalisation can also produce new forms of inequality. Individuals differ in access to reliable internet connections, suitable devices, digital literacy, language skills, and the ability to understand complex online instructions. Persons with disabilities may face inaccessible interfaces, while older citizens may depend on family members or private intermediaries to complete sensitive administrative processes. Ranchordas observes that digital welfare administration may transform socioeconomic inequality into

administrative exclusion when access to public rights depends on technological competence (Ranchordas, 2023). Formal availability of an online service is therefore insufficient. Equal access requires reasonable accommodation, accessible design, assisted-digital support, alternative channels, and procedures for those who cannot use standardised electronic systems.

The protection of privacy and personal data forms a further normative pillar. Digital government depends on the collection, storage, linkage, and analysis of extensive information about citizens. Such information may include identity records, financial data, family relationships, health information, educational history, employment status, geographic location, and patterns of interaction with public institutions. The concentration of these datasets can improve administrative coordination and reduce repeated requests for information, but it also increases the state's capacity to monitor, categorise, and profile individuals. Bannister and Connolly argue that public-sector information systems should be evaluated against public values such as privacy, fairness, accountability, and trust, even where the systems generate operational benefits (Bannister & Connolly, 2014). Rights-based data governance therefore requires limitation of collection, defined purposes, controlled access, accuracy, secure retention, transparent sharing, and effective mechanisms for correction and deletion where legally appropriate.

Data security is closely related to privacy but should not be treated as identical. Privacy concerns the legitimate scope and purpose of governmental access to information, while security concerns protection against unauthorised access, alteration, loss, or disruption. An institution may collect information lawfully but fail to secure it adequately. Conversely, a highly secure system may still violate privacy by gathering excessive data or using it for unrelated purposes. The increasing interconnection of administrative systems magnifies both types of risk. A security failure in one institution may compromise data used by several others, while a mistaken entry may propagate across interconnected databases. Wirtz emphasises that the reliability of automated public-sector systems depends heavily on the quality, integrity, and governance of their underlying data (Wirtz et al., 2019). Rights-based governance must consequently regulate the entire lifecycle of administrative information, including collection,

verification, sharing, correction, retention, access control, and destruction.

Transparency in digital administration also requires reinterpretation. Traditional administrative transparency focuses on access to documents, publication of rules, disclosure of procedures, and provision of reasons. In algorithmic or data-driven administration, formal disclosure may not provide meaningful understanding. A public authority might publish a technical description of a system that ordinary citizens cannot interpret, or provide a generic explanation that does not reveal why a particular person received a particular outcome. Ranchordas identifies this problem in automated welfare systems, where citizens may formally receive a decision but remain unable to understand the data or classifications that produced it (Ranchordas, 2023). Meaningful transparency requires information to be provided in an intelligible, relevant, and contestable form. Citizens should know which data were used, what legal criteria applied, whether automation influenced the outcome, and how an error can be corrected.

Accountability refers to the obligation of public authorities to explain, justify, and accept responsibility for their actions. Digital systems can strengthen accountability by creating electronic records, standardising procedures, and enabling audit trails. They may also weaken it by dispersing decision-making across administrative units, technological providers, and automated processes. Ghazi Shariat-Panahi explains that administrative accountability depends on the ability to attribute governmental action to a legally responsible authority (Ghazi Shariat-Panahi, 2025). This principle cannot be displaced by technological complexity. A public institution should not be permitted to claim that a harmful decision was produced by “the system” as though the system were an autonomous legal actor. Responsibility must remain with the authority that selected, deployed, supervised, and relied on the technology. Private contractors may bear contractual or professional obligations, but the public body remains responsible for ensuring that governmental authority is exercised lawfully.

The right to challenge an administrative decision is equally fundamental. Administrative justice requires more than the availability of a formal appeal procedure. Citizens must be able to obtain relevant information,

present evidence, correct inaccurate data, and receive reconsideration by a competent human authority. Ranjbar’s analysis of administrative justice emphasises the importance of institutional mechanisms capable of reviewing administrative legality, correcting errors, and protecting individuals against unlawful exercises of public power (Ranjbar, 2016). In a digital environment, these mechanisms must address errors that may originate in data collection, identity matching, automated classification, software design, or inter-agency communication. An appeal system that merely reproduces the original automated outcome cannot provide effective review. Human reconsideration must be genuine, informed, and authorised to depart from the system’s recommendation where legal or factual circumstances require it.

The concept of rights-based digital governance brings these principles together. It treats e-government as a multilayered structure in which digital services, data-driven administration, interoperability, electronic participation, and automation operate under a normative framework composed of legality, transparency, accountability, equality, privacy, data security, proportionality, access, and effective remedy. This model does not assume that administrative efficiency and citizens’ rights are inherently opposed. On the contrary, accurate data, transparent procedures, accessible services, and effective complaint mechanisms can improve both efficiency and legitimacy. A system that enables citizens to correct their information before a decision is made may reduce appeals and administrative costs. A transparent allocation rule may improve public confidence and reduce disputes. A well-designed accessible service may expand usage while decreasing dependence on expensive physical procedures. Rights can therefore function as design requirements that improve administrative performance rather than as external obstacles imposed after technological development.

Proportionality is especially important in reconciling administrative objectives with individual rights. Governmental data collection, identity verification, surveillance, and automation should not exceed what is necessary to achieve a legitimate public purpose. Fertikh’s examination of administrative power and social rights illustrates the continuing need to balance governmental capacity with legal protections for

individuals who depend on public institutions (Fertikh, 2025). In digital administration, proportionality requires authorities to consider whether less intrusive methods could achieve the same objective, whether the benefits of integration justify privacy risks, and whether full automation is appropriate for decisions with serious consequences. It also requires differentiated safeguards according to the significance of the decision. An automated appointment-booking system does not demand the same level of explanation and review as an automated decision denying essential social support.

Public trust is the final connecting element of the framework. Trust is not generated merely by technological sophistication or the speed of digital transactions. It emerges when citizens believe that institutions are competent, lawful, secure, fair, and responsive. Bannister and Connolly emphasise that public value in digital government includes legitimacy and confidence, not only productivity (Bannister & Connolly, 2014). Repeated system failures, unexplained decisions, privacy violations, or inaccessible complaint mechanisms can undermine trust even when most transactions are completed successfully. Conversely, public institutions that acknowledge errors, provide clear information, preserve human assistance, and demonstrate effective oversight may build trust despite technical limitations. Rights-based digital governance therefore evaluates digital transformation according to the combined outcome of efficient public administration and sustainable protection of citizens' public rights.

3. Legal and Institutional Contexts of E-Government in Iran and the United Kingdom

The legal and institutional context of Iran reflects a public-administration system in which digital transformation has developed through numerous sectoral programmes, administrative portals, integrated databases, and national initiatives aimed at reducing physical bureaucracy and expanding electronic access to governmental services. The Iranian administrative system has historically been characterised by a relatively centralised legal structure combined with substantial organisational fragmentation in implementation. Ministries, public organisations, municipalities, regulatory institutions, and specialised bodies exercise distinct competences and maintain their own information systems. This combination means that

digital reform often proceeds through separate institutional projects rather than through a fully integrated administrative architecture. Tabatabaei Motameni explains that the distribution of administrative competence in Iran is shaped by legal hierarchy, institutional specialisation, and the relationship between central and decentralised public bodies (Tabatabaei Motameni, 2020). These features affect digital transformation because technological integration requires not only compatible software but also clear authority for information exchange, standardised procedures, and agreed allocation of institutional responsibility.

Iranian e-government initiatives have created significant opportunities for citizens to access public services remotely, submit applications electronically, obtain administrative information, make digital payments, and follow the progress of certain procedures. These developments can reduce travel, waiting times, direct administrative contact, and opportunities for informal interference. Shakeri's early analysis of e-government in Iran identified service accessibility, reduction of administrative expenses, and improvement of government-citizen communication as central anticipated benefits (Shakeri, 2011). The rapid expansion of digital services has subsequently confirmed the practical importance of these capacities. Nevertheless, the existence of electronic channels does not necessarily indicate full digital integration. Citizens may still be required to use several platforms, enter the same information repeatedly, obtain physical confirmation from another authority, or attend an office when electronic systems cannot process exceptional cases. The resulting model may be partly digital but remain institutionally fragmented.

One central legal issue in Iran is the relationship between digital administrative practices and the traditional principles of administrative law. Administrative bodies must act within legally defined competences and follow procedures established by law or valid regulation. Abbasi emphasises that administrative legality requires both a substantive legal basis and observance of procedural standards designed to protect individuals (Abbasi, 2025). Digital systems, however, are frequently developed as technical projects before all of their legal implications have been comprehensively addressed. An institution may connect databases because doing so

appears administratively useful, while questions concerning the scope of authorised data sharing, retention, citizen notification, and responsibility for inaccuracies remain unresolved. Similarly, online procedures may be introduced without clearly specifying the legal status of electronic communications, the moment at which a decision becomes effective, or the appropriate remedy when a system fails.

The absence of a fully integrated and comprehensive approach to personal-data governance is especially important. Iranian public bodies hold substantial quantities of personal information, and the expansion of interoperability increases the possibility that information collected for one administrative purpose will be used for another. Gorji Azandariani's account of public-law foundations indicates that the exercise of public authority must remain limited by respect for individual rights and the public interest (Gorji Azandariani, 2016). In the digital environment, this requires clear rules concerning data minimisation, purpose limitation, institutional access, accuracy, retention, security, and accountability. Fragmented regulation creates uncertainty for both citizens and administrators. Citizens may not know which authority holds particular information or how to correct it, while public institutions may lack consistent standards for lawful sharing and security.

The Iranian institutional environment also displays unequal levels of digital maturity. Some public institutions possess advanced technical infrastructure and specialised staff, while others rely on outdated systems, limited connectivity, or manual procedures. This unevenness weakens interoperability and may create unequal access to public services according to location or administrative sector. Alvani notes that organisational reform depends on human resources, institutional culture, managerial capacity, and coordination, not merely on formal plans or technological investment (Alvani, 2016). Digital transformation in Iran is therefore affected by resistance to organisational change, insufficient training, uncertainty concerning new responsibilities, and the tendency to preserve conventional procedures within electronic interfaces. Where staff members do not trust the system or lack authority to correct its outputs, citizens may be required to navigate both digital and traditional bureaucracy simultaneously.

Administrative justice constitutes another central element of the Iranian context. Citizens who are harmed by administrative action may seek review through internal administrative mechanisms, supervisory institutions, or judicial bodies, including administrative-justice structures. Ranjbar emphasises that effective administrative justice requires accessible procedures, institutional independence, and the practical capacity to correct unlawful decisions (Ranjbar, 2016). Digital administration creates new challenges for these mechanisms. A claimant may need access to technical logs, database histories, automated classifications, or information held by multiple institutions. Courts and review bodies may face difficulty identifying the source of an error or determining whether a decision was made by an official or generated automatically. Traditional review procedures remain essential, but they must develop the capacity to examine digital evidence and allocate responsibility within complex technological systems.

The United Kingdom presents a different institutional setting. Its digital-government model has generally placed greater emphasis on common service standards, central guidance, user-oriented design, accessibility, and coordination across public institutions. Digital transformation has been incorporated into broader administrative-reform strategies rather than treated solely as a technical matter. Bannister and Connolly's public-value framework reflects an important dimension of the British and European administrative debate: digital projects should be assessed according to their contribution to transparency, fairness, responsiveness, trust, and democratic legitimacy, not only their efficiency (Bannister & Connolly, 2014). This orientation has encouraged stronger attention to the experience of service users, simplification of procedures, and consistent design across governmental platforms.

The United Kingdom's more developed legal culture of data protection, freedom of information, equality, and administrative review provides comparatively stronger safeguards for citizens. These safeguards do not eliminate digital risks, but they create a more structured framework within which public institutions must justify information processing, accommodate accessibility needs, and respond to challenges. Fertikh's examination of administrative power and social rights demonstrates that modern administrative systems must reconcile

institutional efficiency with legal obligations toward individuals who depend on public services (Fertikh, 2025). This is especially relevant in the United Kingdom because digital administration is deeply embedded in welfare provision, taxation, immigration, healthcare, local-government services, and regulatory systems. The legal framework imposes constraints, yet the scale and complexity of digital government continually test the effectiveness of those constraints.

A defining strength of the British model is its emphasis on service design from the perspective of the user. Rather than merely converting existing forms into electronic formats, digital reform frequently seeks to simplify the entire administrative journey. Mergel's conception of digital transformation supports this process-oriented approach by emphasising organisational redesign and user-centred innovation (Mergel et al., 2019). Such an approach can reduce unnecessary information requests, combine related services, and create clearer communication. However, user-centred design may still fail when the "typical user" imagined by designers does not reflect the diversity of actual citizens. Individuals with disabilities, unstable housing, limited literacy, irregular immigration status, or complex family circumstances may not fit standardised digital pathways. The English experience therefore demonstrates both the value and the limitations of user-centred administrative reform.

The United Kingdom has also experienced significant controversy concerning digital welfare and automated administration. Ranchordas argues that digital welfare states may subject access to social rights to technical processes that are difficult for claimants to understand or contest (Ranchordas, 2023). Automated verification, risk assessment, and data matching may increase the speed and consistency of decisions, but they can also intensify surveillance and create harsh consequences when information is inaccurate. Individuals dependent on public benefits are particularly vulnerable because delays or errors may affect their ability to meet essential needs. The existence of more developed legal safeguards does not guarantee that citizens can effectively use them. Complex complaint processes, limited legal assistance, and informational asymmetry may still prevent meaningful challenge.

Outsourcing and networked administration create additional accountability issues in the United Kingdom.

Public services may depend on private technology companies, consultancy firms, platform providers, and data processors. The involvement of specialised contractors can improve technical capacity but may make responsibility more difficult to identify. Wirtz notes that public-sector use of artificial intelligence and advanced technologies requires clear governance structures, institutional expertise, and accountability arrangements (Wirtz et al., 2019). A public authority cannot avoid responsibility by attributing a harmful outcome to a proprietary system or private supplier. Yet commercial confidentiality may limit disclosure of technical details, while fragmented contracts may make it difficult to determine which actor caused an error. This problem is less visible in systems where technology is understood as an internal administrative tool, but it becomes central when governmental authority is exercised through complex public-private networks.

The comparison between Iran and the United Kingdom reveals both structural differences and common pressures. Iran's principal challenges arise from incomplete integration, legal fragmentation, unequal institutional capacity, and limited rights-oriented regulation of data-driven administration. The United Kingdom possesses stronger institutional coordination and more developed legal safeguards, but its extensive reliance on digital systems produces advanced forms of risk, including automated exclusion, large-scale data integration, and dispersed responsibility. Doan's analysis indicates that digital administrative reform succeeds only when technological innovation is accompanied by institutional capacity, clear governance, and responsiveness to social conditions (Doan, 2025). This proposition applies to both systems, although the specific weaknesses differ.

The concept of administrative culture is essential to understanding these differences. In Iran, digitalisation frequently occurs within a bureaucratic culture that values formal compliance, documentary proof, hierarchical approval, and institutional control. Technology may therefore be used to reinforce existing administrative practices rather than question their necessity. In the United Kingdom, reform discourse more strongly emphasises service design, user experience, and performance measurement, but this culture may prioritise standardisation and measurable outputs in ways that marginalise complex individual

circumstances. Alvani's analysis of public management demonstrates that organisational values and managerial assumptions shape how administrative reforms are implemented (Alvani, 2016). Technology does not independently determine outcomes; it reflects the institutional priorities embedded in its design and use.

The role of public-law review also differs. Iran's system contains formal mechanisms of administrative supervision and judicial review, but effective challenge may be hindered by limited transparency, difficulties in obtaining administrative information, and uncertainty regarding digital evidence. The United Kingdom possesses a comparatively established culture of reason-giving, ombudsman review, judicial scrutiny, and public accountability, but claimants may still encounter procedural complexity and resource barriers. Ghazi Shariat-Panahi underlines that administrative accountability is effective only when legal responsibility can be connected to practical review and enforceable consequences (Ghazi Shariat-Panahi, 2025). Both countries therefore require review mechanisms that are specifically capable of examining digital systems rather than treating technological decisions as ordinary administrative acts whose underlying processes are presumed to be accessible.

The comparison should not lead to mechanical legal transplantation. Institutional arrangements that operate within the United Kingdom depend on its administrative traditions, professional capacities, legal remedies, regulatory institutions, and political culture. Importing isolated technological or legal mechanisms into Iran without addressing institutional fragmentation and administrative capacity would be unlikely to produce equivalent results. Xu's law-based governance approach indicates that reform must align technological change with the specific legal structure and institutional conditions of the jurisdiction concerned (Xu, 2024). The relevant lesson from the English experience is therefore not the replication of individual platforms or procedures but the adoption of broader principles: coherent coordination, clear allocation of responsibility, user-centred process redesign, accessible alternative channels, strong data governance, meaningful transparency, and effective review.

A rights-based comparison ultimately reveals that digital-government maturity should not be measured only by the quantity of online services or the

sophistication of technological infrastructure. A legally mature system is one in which citizens can understand how public authority is exercised, access services without discrimination, protect and correct their information, receive meaningful reasons, obtain human assistance, and challenge unlawful outcomes. Bannister and Connolly's emphasis on public values provides a common evaluative standard for both countries (Bannister & Connolly, 2014). Iran may improve efficiency through integration and simplification, while the United Kingdom may need stronger controls over automation and outsourcing. In both systems, the decisive question is whether institutional design ensures that technology remains an accountable instrument of public administration rather than an opaque source of administrative power.

4. Comparative Analysis of the Challenges of E-Government

The first major challenge concerns institutional fragmentation and weak interoperability. E-government can improve administrative efficiency only when public bodies are capable of exchanging accurate information through legally authorised and technically compatible systems. In fragmented environments, each institution may establish its own portal, authentication process, database, and documentary requirements. Citizens then face multiple digital entry points and may be required to provide the same information repeatedly. This undermines one of the primary promises of digital government: that information already held by the state should not need to be resubmitted unnecessarily. In Iran, institutional fragmentation is intensified by differences in administrative capacity, inconsistent technical standards, and uncertainty concerning the legal authority to share information. Tabatabaei Motameni's analysis of administrative organisation shows that the distribution of public functions among numerous specialised institutions requires clear coordination and competence rules (Tabatabaei Motameni, 2020). Where those rules are unclear, technological integration may either remain incomplete or proceed without adequate legal safeguards.

Interoperability is not merely a technical matter. It requires agreement concerning data definitions, responsibility for accuracy, authorised purposes, security standards, and procedures for correction. A

citizen's address, employment status, family relationship, or financial obligation may be recorded differently across public databases. When systems are connected, inconsistencies may generate erroneous decisions on a larger scale. Wirtz emphasises that the value of data-driven administration depends on the quality and reliability of the information used by public institutions (Wirtz et al., 2019). The United Kingdom has comparatively stronger common standards and more developed coordination, but fragmentation persists among central departments, local authorities, specialised agencies, and contracted service providers. Legacy systems may be technically difficult to integrate, while legal restrictions and institutional caution may impede data sharing. The comparative lesson is that successful interoperability requires a governance framework that combines technical standards with legal responsibility and citizen-accessible correction mechanisms.

A related challenge is the reproduction of bureaucracy in digital form. Administrative digitalisation often begins by transferring existing procedures into online environments without reconsidering whether the procedures themselves are necessary. Paper forms become electronic forms, physical signatures become digital confirmations, and multiple office approvals become sequential online authorisations. Mergel's research demonstrates that digital transformation differs from simple digitisation because it requires the redesign of organisational processes and service models (Mergel et al., 2019). In Iran, many services remain shaped by documentary and hierarchical administrative traditions. Citizens may upload documents that another public body already possesses, enter information already stored in governmental databases, or complete online procedures that still require physical verification. The result is a hybrid bureaucracy that combines the burdens of digital and conventional administration.

The United Kingdom's stronger emphasis on user-centred design provides a partial response to this problem. Administrative procedures may be redesigned around the citizen's objective rather than the internal structure of government. Nevertheless, standardised digital pathways can create their own rigidity. A process designed for the majority may be unable to accommodate exceptional evidence, unusual family arrangements, or complex legal status. Bannister and

Connolly warn that digital-government transformation should not be evaluated solely by streamlined service delivery because standardisation may conflict with fairness, inclusiveness, and other public values (Bannister & Connolly, 2014). Both countries therefore face the challenge of simplifying ordinary procedures without eliminating the flexibility necessary for lawful individualised administration.

Human resources and organisational resistance constitute another major obstacle. Digital systems change the roles of public employees, redistribute authority, and require new forms of expertise. Officials may resist systems that reduce their discretion, alter established workflows, or expose their performance to greater monitoring. Alternatively, they may rely too heavily on automated outputs because they lack confidence or training to question them. Alvani explains that organisational change requires leadership, participation, professional development, and alignment between technological reform and institutional culture (Alvani, 2016). In Iran, unequal training and resource constraints mean that some public bodies cannot fully operate or maintain advanced systems. Staff may continue parallel paper procedures as a precaution, reducing anticipated efficiency. In the United Kingdom, greater professional digital capacity exists, but shortages of specialised expertise and dependence on contractors may still weaken institutional control.

The relationship between public officials and technological systems is particularly important. Automation should support administrative judgment rather than eliminate legally required discretion. If officials treat a system-generated recommendation as binding, the practical decision may be made by technical rules that were never formally authorised as law. Abbasi's discussion of administrative discretion indicates that public officials must exercise legally conferred judgment in accordance with relevant purposes, evidence, and procedural fairness (Abbasi, 2025). A digital system may organise evidence or identify patterns, but it cannot lawfully replace discretion where the legal framework requires consideration of individual circumstances. Both Iran and the United Kingdom need clear rules defining when automation is advisory, when it is determinative, and who bears responsibility for reviewing its output.

Infrastructure failure and cybersecurity present simultaneous efficiency and rights-related risks. As public services become dependent on digital platforms, system outages may prevent citizens from accessing essential services, submitting time-sensitive applications, making payments, or exercising procedural rights. The concentration of information also creates attractive targets for cyberattacks. Security failures may expose personal data, disrupt public functions, corrupt records, or undermine confidence in governmental institutions. Wirtz identifies cybersecurity, technological reliability, and institutional preparedness as central challenges in public-sector adoption of advanced digital systems (Wirtz et al., 2019). In Iran, infrastructure inequality, connectivity problems, system instability, and external technological constraints may reduce service continuity. In the United Kingdom, more advanced infrastructure provides greater capacity but also creates extensive dependence on complex networks and third-party suppliers.

Administrative resilience should be understood as a public-law obligation rather than merely a technical objective. When access to a legal entitlement depends on a digital platform, the state must provide reasonable arrangements for periods of disruption. A citizen should not lose a right because an online system was unavailable before a deadline. Ghazi Shariat-Panahi's account of administrative responsibility supports the principle that public authorities remain accountable for failures in the organisation of public services (Ghazi Shariat-Panahi, 2025). Resilient e-government therefore requires backup systems, alternative communication channels, transparent incident reporting, extended deadlines where appropriate, secure recovery procedures, and clear responsibility for compensating or correcting harmful consequences.

Data quality is another foundational challenge. Digital systems often create an appearance of objectivity because information is processed automatically and decisions are generated consistently. Yet automated consistency can reproduce inaccurate information more rapidly and extensively than traditional administration. An error in identity data, employment records, family status, tax information, or previous administrative decisions may affect several services once databases are integrated. Ranchordas demonstrates that data errors in digital welfare systems can produce serious

consequences because automated processes may treat recorded information as unquestionably valid (Ranchordas, 2023). Citizens may find it difficult to determine which authority created the error or which database must be corrected.

Iran's fragmented administrative structure increases the risk that inconsistent information will remain distributed across multiple systems. Correcting one record may not automatically correct related records held elsewhere. The United Kingdom's more integrated systems may reduce repeated data entry but increase the consequences of centralised error. The greater the degree of interoperability, the more important it becomes to establish rights of access, correction, notification, and traceability. Doan's analysis of digital administrative services confirms that data integration must be supported by governance arrangements capable of ensuring accuracy, institutional coordination, and responsive service delivery (Doan, 2025). Both systems need mechanisms allowing citizens to identify the source of information, understand how it has been used, and obtain timely correction across connected institutions.

The digital divide represents one of the most visible threats to equal access. Digital services can benefit citizens who live far from administrative centres, have mobility limitations, or require access outside working hours. However, these benefits depend on internet availability, digital devices, literacy, language, disability accommodation, and confidence in using electronic systems. Ranchordas argues that digital welfare systems may create a new form of administrative conditionality in which access to social rights depends on digital competence (Ranchordas, 2023). In Iran, geographic inequalities in connectivity, differences in household resources, and uneven digital literacy may particularly affect rural residents, older persons, low-income households, and marginalised groups. The existence of a national digital portal does not establish equality when substantial sections of the population cannot use it independently.

The United Kingdom also faces digital exclusion despite stronger infrastructure. Older citizens, persons with disabilities, individuals experiencing homelessness, migrants with limited language skills, and people without stable internet access may struggle with digital-only procedures. User-centred design can improve accessibility, but it cannot eliminate socioeconomic

barriers. Fertikh's analysis of social rights and administrative power indicates that public institutions have a heightened responsibility toward individuals whose dependency on administrative systems makes exclusion particularly harmful (Fertikh, 2025). Assisted-digital services, telephone access, face-to-face alternatives, accessible design, and support through trusted intermediaries should therefore be treated as integral parts of e-government rather than temporary exceptions.

Digital exclusion may also arise from procedural complexity rather than lack of equipment. A citizen may possess a smartphone and internet access but still be unable to understand legal terminology, upload documents in required formats, navigate identity verification, or respond to automated notifications. Formal digital access must be distinguished from effective administrative access. Gorji Azandariani's public-law framework supports the principle that equality requires attention to the practical effects of governmental procedures, not merely formally identical rules (Gorji Azandariani, 2016). A single digital procedure applied to everyone may produce discriminatory outcomes when individuals possess substantially different capacities to comply.

Privacy and the concentration of informational power constitute another major comparative concern. E-government encourages public bodies to gather and connect information in order to provide coordinated services, detect fraud, plan resources, and personalise administrative interactions. These objectives may be legitimate, but extensive data integration can create detailed profiles of citizens and expand the capacity for monitoring. Bannister and Connolly identify privacy as a core public value that may conflict with the efficiency and integration objectives of digital government (Bannister & Connolly, 2014). In Iran, incomplete and dispersed data-protection rules may create uncertainty concerning the permissible scope of inter-agency sharing and the rights of individuals. Citizens may receive limited information about why data are collected, how long they are retained, or which institutions can access them.

The United Kingdom provides stronger formal data-protection safeguards, but large-scale administrative data use continues to raise concerns. Legal compliance may become procedural rather than substantive if

authorities rely on broad public-interest grounds without carefully examining necessity and proportionality. The use of data for purposes different from those originally communicated may undermine trust even when it is technically lawful. Xu's emphasis on law-based administrative governance supports the requirement that governmental data practices remain connected to defined legal purposes and subject to effective oversight (Xu, 2024). Privacy protection must therefore involve more than cybersecurity. It requires limits on collection, linkage, profiling, reuse, retention, and disclosure.

Algorithmic decision-making intensifies these concerns. Public institutions increasingly use automated systems to rank applications, identify suspicious behaviour, allocate inspections, calculate entitlements, or recommend decisions. Such systems may improve consistency and allow administrators to process large volumes of information. Wirtz notes that artificial intelligence can support public-sector efficiency through prediction, classification, and automated analysis (Wirtz et al., 2019). Yet the same systems may reproduce historical bias, rely on incomplete data, or employ criteria that are difficult to justify legally. An algorithm does not need to use an explicitly discriminatory variable to produce unequal effects; correlations with location, income, employment history, language, or family circumstances may indirectly disadvantage particular groups.

The challenge of algorithmic discrimination is greater when the system is opaque. Citizens may not know that automation influenced a decision, and officials may be unable to explain the model's operation. Ranchordas shows that algorithmic welfare administration can weaken rights by making adverse outcomes difficult to understand and contest (Ranchordas, 2023). In Iran, algorithmic governance remains less institutionally developed, but increasing data integration and automated administrative processes make early legal regulation essential. The United Kingdom has more extensive experience with automated public decision-making and therefore demonstrates both the potential benefits and the practical difficulty of ensuring transparency, fairness, and human review.

The principle of explainability should not be interpreted as requiring every citizen to understand complex computer code. What matters is whether the authority

can provide an intelligible explanation of the relevant factors, data, legal criteria, and reasoning. Abbasi's account of administrative procedure supports the requirement that public decisions be reasoned and reviewable (Abbasi, 2025). If an authority cannot explain why a system produced a particular result, it should not rely on that result to impose a significant burden or deny a legal benefit. Technical complexity is not a lawful substitute for reasons.

Accountability becomes difficult when digital administration is distributed across several institutions and private actors. A harmful outcome may result from inaccurate data supplied by one body, software designed by another, rules specified by a third, and a final decision formally issued by a fourth. Ghazi Shariat-Panahi emphasises that administrative responsibility requires identifiable attribution of public action (Ghazi Shariat-Panahi, 2025). Citizens should not be expected to investigate complex institutional relationships before obtaining correction or remedy. The public authority communicating the decision should accept initial responsibility for resolving the problem, even where it later seeks contribution from another institution or contractor.

Private-sector involvement creates particular challenges in the United Kingdom, where governmental digital projects may rely on external providers. Proprietary systems may restrict access to technical information, and contractual arrangements may divide responsibility in ways that are invisible to citizens. Iran also uses private contractors, but weaker transparency and procurement oversight may make responsibility even more difficult to trace. Bannister and Connolly's public-value approach requires public institutions to ensure that outsourcing does not reduce transparency, accountability, or control over public data (Bannister & Connolly, 2014). Public authority cannot be contractually delegated in a manner that deprives citizens of legal protection.

Transparency may be strengthened by digitalisation because electronic systems create records of submissions, decisions, communications, and modifications. These records can support audit, supervision, and anti-corruption measures. Yet digital transparency is not automatic. Public institutions may collect extensive information about citizens while revealing little about their own systems. This asymmetry creates a situation in which government becomes

increasingly capable of observing the public while remaining technologically opaque. Gorji Azandariani's analysis of public law indicates that transparency functions as a constraint on power and a condition of legitimate administration (Gorji Azandariani, 2016). Rights-based digital governance therefore requires publication of relevant rules, system purposes, institutional responsibilities, data-sharing arrangements, and procedures for challenge.

The ability to appeal and obtain effective remedy is a decisive test of digital administration. A citizen harmed by an erroneous digital decision must be able to identify the decision, understand its basis, submit relevant evidence, obtain human reconsideration, and secure correction within a reasonable time. Ranjbar emphasises that administrative justice must provide practical protection against unlawful administrative action rather than merely formal access to review institutions (Ranjbar, 2016). In Iran, digital complaint systems may improve access, but legal and technical complexity may prevent claimants from obtaining the information necessary to prove an error. Courts and review bodies require expertise to examine digital records and understand automated processes.

The United Kingdom possesses more established complaint, ombudsman, and judicial-review mechanisms, but procedural availability does not guarantee substantive accessibility. Individuals affected by welfare automation or complex data matching may lack legal assistance, technical knowledge, or resources. Fertikh's analysis of administrative power and social rights illustrates how procedural barriers can weaken the effective protection of rights even in developed legal systems (Fertikh, 2025). Effective remedy should therefore be designed into the administrative system. Institutions should identify and correct errors proactively, provide simple internal review, preserve relevant logs, and suspend harmful consequences where a credible challenge is pending.

The decline of human assistance is a further challenge shared by both jurisdictions. Digital government is frequently justified as a means of reducing the need for public employees to perform routine tasks. This can allow staff to focus on complex cases, but only if institutions preserve accessible human channels. In practice, digitalisation may lead to office closures, reduced telephone support, and dependence on

automated responses. Citizens whose circumstances do not fit standard categories may become trapped within systems that repeatedly reject their submissions without explaining how the problem can be resolved. Alvani's public-management perspective indicates that administrative quality depends on responsiveness and the ability of organisations to address real human needs (Alvani, 2016). Human assistance should consequently be viewed as an essential component of digital service design.

The Iranian context makes human support particularly important because digital literacy and infrastructure are uneven. Eliminating physical channels too quickly may exclude substantial groups. In the United Kingdom, digital-first policies may similarly disadvantage citizens requiring personalised assistance. Ranchordas warns that digital welfare systems can depersonalise the administration of social rights and place excessive responsibility on claimants to navigate technical processes (Ranchordas, 2023). A rights-based model should use automation for routine tasks while guaranteeing access to a responsible official when legal interests are significantly affected.

Public trust synthesises all of these challenges. Citizens are more likely to use digital services when they believe that systems are reliable, information is secure, decisions are fair, and institutions will respond when errors occur. Trust may be damaged by system outages, data breaches, unexplained decisions, inaccessible procedures, or the perception that digitalisation is primarily intended to increase governmental control. Bannister and Connolly identify trust and legitimacy as fundamental public values in digital transformation (Bannister & Connolly, 2014). Iran's digital-government development may be undermined if rapid technological expansion is not accompanied by transparent safeguards and credible accountability. The United Kingdom's stronger institutional framework may support greater trust, but controversies concerning surveillance, automated welfare decisions, and data sharing demonstrate that trust must be continually earned.

The comparative analysis indicates that the two systems face similar categories of risk but differ in the maturity of their responses. Iran's challenges are more strongly associated with fragmented legal regulation, uneven institutional capacity, incomplete interoperability, limited transparency, and weakly developed data-

governance safeguards. The United Kingdom's challenges arise within a more integrated and legally regulated system but involve advanced forms of automation, outsourcing, digital exclusion, and informational concentration. Mergel's account of digital transformation confirms that technological maturity creates organisational and governance challenges rather than eliminating them (Mergel et al., 2019). The United Kingdom cannot therefore be treated as an endpoint toward which Iran should move uncritically. Its experience provides lessons concerning coordination, service design, accessibility, and review, but also warnings concerning excessive automation and digital dependency.

A balanced model for Iran should combine administrative simplification with rights-oriented institutional reform. Interoperability should be developed through clear legal authority, defined responsibility, and common data standards. Digital services should be designed around citizens' needs rather than the internal boundaries of public bodies. Personal information should be collected and shared only for defined purposes. Significant automated decisions should remain subject to human review and meaningful explanation. Alternative channels should be preserved for citizens unable to use digital services. Administrative-review institutions should acquire the capacity to examine technological systems and order effective correction. These reforms would not merely protect rights; they would improve efficiency by reducing errors, repeated applications, complaints, and institutional conflict.

The United Kingdom should similarly continue to strengthen oversight of automated systems, public-private digital partnerships, and digital welfare administration. Greater transparency concerning algorithms, stronger assessment of discriminatory effects, accessible human support, and effective remedies remain necessary. Wirtz's analysis demonstrates that advanced technological use in the public sector requires continuous governance, evaluation, and institutional learning (Wirtz et al., 2019). Digital-government reform is not a one-time transition but an ongoing process in which legal safeguards, administrative capacities, and technological systems must evolve together.

The central finding is that administrative efficiency and citizens' public rights are not independent outcomes. Fragmented systems, inaccurate data, inaccessible procedures, and weak accountability reduce both. Conversely, lawful data governance, transparent processes, accessible service design, and effective review improve both administrative performance and public legitimacy. Rights-based digital governance should therefore serve as the framework through which digital initiatives are planned, implemented, evaluated, and revised. Technology is the starting point of digital administration, but the legitimacy and success of e-government depend on the legal and institutional structure within which that technology operates.

5. Conclusion

E-government has become an indispensable component of contemporary public administration. Governments can no longer respond effectively to complex social needs, expanding service demands, limited public resources, and increasing expectations of accessibility through exclusively paper-based and office-centred procedures. Digital systems offer substantial capacity to accelerate services, reduce repetitive administrative work, improve communication, coordinate public institutions, enhance the use of information, and make administrative processes more accessible. Nevertheless, the movement from traditional administration to digital administration does not automatically create a more efficient, lawful, or citizen-centred state. Technology can simplify procedures, but it can also conceal administrative complexity. It can reduce direct contact, but it can also isolate citizens from responsible officials. It can improve consistency, but it can also reproduce errors and inequalities on a larger scale. The ultimate effects of e-government depend on the legal, institutional, managerial, and ethical framework governing its use.

The comparative examination of Iran and the United Kingdom demonstrates that digital-government challenges arise at different stages of institutional development. Iran has made significant progress in expanding electronic services and creating digital channels through which citizens can interact with public institutions. These developments have reduced some traditional administrative burdens and increased the accessibility of numerous public services. Yet

technological expansion has not always been accompanied by equivalent development in legal coordination, organisational integration, data governance, administrative accountability, and procedural protection. Fragmented platforms, repeated documentary requirements, unequal technological capacity among public bodies, unstable infrastructure, unclear responsibility, and incomplete protection of personal information limit the transformative effect of e-government. In many cases, technology has been added to existing bureaucracy without sufficient reconsideration of the procedures, competencies, and institutional relationships underlying it.

The United Kingdom possesses a more mature digital-administration environment, stronger traditions of service standardisation, comparatively developed data-protection principles, and more accessible mechanisms of administrative review. Its experience demonstrates the benefits of central coordination, common service standards, user-oriented design, and systematic attention to accessibility. However, it also shows that technological maturity does not eliminate risks. The greater integration of governmental systems increases the consequences of data errors and cybersecurity failures. Extensive automation may make public services less responsive to exceptional circumstances. Digital welfare administration may exclude individuals who lack technological resources or skills. Outsourcing may obscure responsibility, and the use of proprietary systems may limit meaningful transparency. The British experience should therefore be understood as both a source of institutional lessons and a warning against equating advanced technology with rights-compatible administration.

The principal conclusion of this article is that administrative efficiency and the safeguarding of citizens' public rights must be pursued through a single integrated framework. Efficiency should not be measured only by speed, cost reduction, transaction volume, or the number of services placed online. A digital administrative system is efficient only when it provides accurate, reliable, accessible, continuous, and legally defensible services. A decision that is generated rapidly but based on incorrect information is not efficient. A platform that reduces governmental expenditure while imposing excessive burdens on citizens is not efficient. An automated process that cannot explain or correct its

outcome is not efficient. Genuine administrative efficiency includes the capacity to prevent mistakes, accommodate individual circumstances, resolve complaints, maintain public trust, and achieve lawful public purposes.

Citizens' public rights should similarly be understood as operational requirements of digital administration rather than abstract limitations imposed after technological systems have been created. Equality requires accessible design, assisted-digital support, and alternative channels. Privacy requires defined purposes, limited collection, controlled sharing, and secure retention. Transparency requires intelligible explanations of procedures, data use, and decision-making criteria. Accountability requires the identification of a legally responsible public authority, even where private contractors or automated systems are involved. Administrative justice requires genuine human reconsideration, access to relevant information, correction of inaccurate data, and effective remedies. These safeguards should be incorporated into the design and procurement of digital systems from the outset.

For Iran, the transition toward rights-based digital governance requires legal consolidation. Public institutions need a coherent framework governing personal-data collection, inter-agency exchange, automated processing, information security, citizen notification, correction rights, and institutional responsibility. Such a framework should define the limits of administrative data use and establish enforceable protections rather than relying exclusively on internal technical policies. Legal reform should also clarify the status of automated decisions, the obligation to provide reasons, the availability of human review, and the responsibility of public bodies for systems developed or operated by private contractors.

Institutional reform is equally necessary. Digital-government responsibilities should be coordinated through common standards while respecting the lawful competences of specialised administrative bodies. Interoperability should not mean unrestricted data exchange; it should mean secure, purpose-specific, accountable, and technically reliable communication between institutions. Each dataset should have an identifiable responsible authority, and citizens should have a clear route for accessing and correcting their information. Institutions should not be permitted to shift

responsibility to one another when integrated systems produce harmful outcomes. The authority communicating or enforcing a decision should ensure that the problem is resolved, even where the underlying error originated elsewhere.

Administrative-process reform should precede or accompany digitalisation. Existing procedures must be examined to determine whether each form, document, approval, and verification remains necessary. Technology should be used to eliminate unnecessary stages rather than merely reproduce them electronically. Public services should be organised around citizens' practical objectives rather than the internal divisions of government. At the same time, simplification should not remove the flexibility required for complex or exceptional cases. Standard digital pathways should include accessible mechanisms for requesting individual consideration and contacting a competent official.

Human resources remain central to successful digital government. Public employees require legal, technical, and ethical training that enables them to understand the operation and limitations of digital systems. Officials should not treat automated outputs as unquestionable. They must retain the authority and professional competence to investigate anomalies, consider individual evidence, and correct errors. Technical experts should work with lawyers, administrators, accessibility specialists, and service users throughout system design. Reliance on private contractors should be accompanied by sufficient internal expertise to supervise contracts, evaluate systems, protect public data, and preserve governmental accountability.

Digital inclusion should be treated as a continuing public responsibility. Governments should not assume that the expansion of internet access eliminates the digital divide. Effective use of administrative systems depends on devices, connectivity, literacy, language, disability accommodation, confidence, and access to assistance. Public bodies should maintain assisted-digital services, telephone support, and face-to-face options where necessary. Alternative access should not be designed as an inferior or punitive route. Citizens using non-digital channels should receive services of comparable quality and should not face unreasonable delays or additional costs.

Automation requires differentiated regulation according to the significance of the decision. Low-risk systems used

for scheduling, information retrieval, or routine communication may require limited safeguards. Systems affecting legal status, social support, taxation, education, healthcare, immigration, regulatory sanctions, or access to essential services require stronger transparency, testing, documentation, and human oversight. Public authorities should assess potential discriminatory effects before deployment and continue monitoring outcomes after implementation. Citizens should be informed when automation materially influences a decision and should be able to obtain an intelligible explanation and human reconsideration.

Cybersecurity and resilience must also be integrated into public-law obligations. Where essential public services depend on digital infrastructure, authorities must prepare for outages, attacks, and data corruption. Backup systems, alternative procedures, incident reporting, secure recovery, and deadline protections should be established in advance. Citizens should not lose entitlements or suffer penalties because a public system was unavailable. Institutions should disclose significant failures, explain remedial measures, and provide compensation or corrective action where service disruption causes unlawful harm.

The United Kingdom's experience suggests that common design standards, central coordination, accessibility requirements, and developed review institutions can substantially improve digital-government quality. Iran can adapt these principles while accounting for its own legal structure, administrative culture, infrastructure, and social conditions. The objective should not be the mechanical importation of foreign platforms or institutional models. Sustainable reform requires domestically appropriate arrangements that connect technology with public-law guarantees and administrative capacity.

The appropriate measure of successful e-government is ultimately whether citizens can receive lawful public services with greater ease, security, equality, and confidence. The number of portals, databases, or automated transactions provides only a partial picture. A successful system enables citizens to understand administrative requirements, submit information without unnecessary repetition, receive accurate decisions within a reasonable time, protect their personal data, obtain human assistance, and challenge errors effectively. It also enables public institutions to

coordinate their activities, use resources responsibly, maintain service continuity, and remain answerable for the exercise of public power.

Rights-based digital governance provides the framework necessary for achieving this result. It rejects both technological determinism and institutional resistance to innovation. Technology is neither an automatic solution nor an unavoidable threat. Its public value depends on how it is designed, governed, supervised, and corrected. When digital transformation is guided by legality, equality, transparency, accountability, privacy, security, proportionality, accessibility, and administrative justice, it can strengthen both governmental capacity and citizens' rights. When these safeguards are absent, digitalisation may simply create a faster, more extensive, and less visible form of bureaucracy. The future of e-government in Iran and the United Kingdom should therefore be directed not merely toward more digital administration, but toward more lawful, inclusive, accountable, resilient, and trustworthy administration.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

- Abbasi, B. (2025). *Administrative Law* (9th ed.). Dadgostar.
- Alvani, S. M. (2016). *Public Management*. Ney Publishing.
- Bannister, F., & Connolly, R. (2014). ICT, Public Values and Transformative Government: A Framework and Programme for Research. *Government Information Quarterly*, 31(1), 119-128. <https://doi.org/10.1016/j.giq.2013.06.002>
- Doan, U. T. T. (2025). Digital Transformation Influencing Civil Administrative Services at Grassroots Governance and Social Development. *The Law and Development Review*. <https://doi.org/10.1515/ldr-2025-0009>
- Fertikh, K. (2025). The Missing Link. International Law, Administrative Power, and European Social Rights. *Historical Social Research/Historische Sozialforschung*, 50(1), 53-73.
- Ghazi Shariat-Panahi, A. (2025). *Administrative Law*. Mizan.
- Gorji Azandariani, A. A. (2016). *Foundations of Public Law*. Jangal Publishing.
- Mergel, I., Edelmann, N., & Haug, N. (2019). Defining Digital Transformation: Results from Expert Interviews. *Government Information Quarterly*, 36(4), 101385. <https://doi.org/10.1016/j.giq.2019.06.002>
- Ranchordas, S. (2023). Digital Welfare States and the Algorithmization of Rights. *German Law Journal*, 24(3), 471-490. <https://doi.org/10.1017/glj.2023.29>
- Ranjbar, A. (2016). *Administrative Justice: Conceptual Framework, Institutional Mechanisms, and Judicial Trends*. Mizan Legal Foundation.
- Shakeri, E. (2011). Electronic Government: Definitions and How It Works. *Hafez*(85), 70-73.
- Tabatabaei Motameni, M. (2020). *Administrative Law*. Organization for Researching and Composing University Textbooks in the Humanities (SAMT).
- Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial Intelligence and the Public Sector: Applications and Challenges. *International Journal of Public Administration*, 42(7), 596-615. <https://doi.org/10.1080/01900692.2018.1498103>
- Xu, J. (2024). Analysis of Law-Based Administrative Law Governance in the Context of the Sharing Economy. *Applied Mathematics and Nonlinear Sciences*, 9(1). <https://doi.org/10.2478/amns-2024-0559>