

DOI: [https://doi.org/10.71317/kjard.2.9\(s\).2026.658](https://doi.org/10.71317/kjard.2.9(s).2026.658)

Kashmir Journal of Academic Research and Development

Journal homepage: <https://rjsaonline.org/index.php/KJARD>

Digital Constitutionalism and Artificial Intelligence Governance: A Comparative Analysis of Pakistan and The United Kingdom

Amna Mumtaz

Ph.D. Law Scholar, International Islamic University, Islamabad

Email: amna.mumtaz11@gmail.com**Adv. Maryam Zahra**

LLM Muslim Family Laws, International Islamic University, Islamabad

Adv. Qasim Shahid

LLM International Commercial Law and Arbitration, University of Hertfordshire

ARTICLE INFO

ABSTRACT

Received:

August 10, 2026

Revised:

August 27, 2026

Accepted:

September 09, 2026

Available Online:

September 22, 2026

Keywords:

Digital Constitutionalism; Artificial Intelligence Governance; Algorithmic Accountability; Data Protection; Privacy Rights; Fundamental Rights; Pakistan; United Kingdom; Automated Decision-Making; AI Regulation.

Corresponding Author:**Amna Mumtaz****Email:**amna.mumtaz11@gmail.com

The rapid expansion of artificial intelligence (AI), algorithmic decision-making, and digital platforms has transformed the relationship between technology, governance, and constitutional rights. While AI systems provide significant opportunities for improving efficiency, public administration, and access to services, they also create complex constitutional challenges concerning privacy, equality, freedom of expression, due process, and accountability. This article examines whether digital constitutionalism can provide an effective framework for governing AI while protecting fundamental rights through a comparative analysis of Pakistan and the United Kingdom. Adopting a doctrinal comparative legal methodology, the study analyses constitutional provisions, legislation, judicial decisions, and policy frameworks relating to digital governance and AI regulation. The research demonstrates that Pakistan possesses important constitutional foundations for digital rights protection, particularly through Articles 9, 10A, 14, 19, and 19A of the Constitution; however, existing legal mechanisms remain fragmented and insufficient for addressing algorithmic surveillance, automated decision-making, and data-driven harms. In contrast, the United Kingdom has developed a more structured approach through the Human Rights Act 1998, UK GDPR, Data Protection Act 2018, and institutional oversight mechanisms. Nevertheless, the UK experience also reveals challenges concerning algorithmic transparency and regulatory adaptation. The article argues that Pakistan requires a context-specific digital constitutionalism model that combines constitutional rights protection with stronger data governance, algorithmic accountability, institutional oversight, and responsible innovation. Rather than restricting technological development, such a framework can ensure that AI adoption remains consistent with democratic values, human dignity, and the rule of law.

Introduction

The rapid advancement of artificial intelligence (AI), automated decision-making systems, and digital platforms has fundamentally transformed the relationship between individuals, governments, and private technological actors. AI is no longer limited to experimental or commercial applications; it increasingly influences public administration, financial services, healthcare, law enforcement, political communication, and judicial decision-making. Through machine learning algorithms, predictive analytics, and data-driven systems, governments and organizations are increasingly able to process large volumes of information and make decisions affecting individuals' rights, opportunities, and access to public services (Wirtz et al., 2019;

Zuiderwijk et al., 2021). While these developments offer significant advantages, including administrative efficiency, improved service delivery, and enhanced decision-making capacity, they also introduce complex constitutional challenges concerning privacy, equality, freedom of expression, transparency, and procedural fairness.

Modern governance is increasingly shaped by algorithmic systems that influence how information is distributed, how risks are assessed, and how decisions are made. Automated decision-making technologies are now used in areas such as welfare administration, policing, employment recruitment, credit assessment, and legal processes. Although these systems are often presented as objective and efficient, scholars have highlighted that algorithms are not inherently neutral because they are developed through human choices, datasets, and institutional assumptions. As a result, AI systems may reproduce existing social inequalities or create new forms of discrimination when biased datasets or opaque decision-making processes are incorporated into technological systems (Noble, 2018; O'Neil, 2016).

The constitutional implications of AI arise because technological systems increasingly affect fundamental rights traditionally protected through constitutional frameworks. Privacy has become particularly significant because AI relies on continuous collection, analysis, and inference from personal information, including identity data, location information, biometric records, financial activities, and behavioral patterns. Unlike traditional privacy violations involving direct intrusion, AI-driven surveillance can operate through large-scale data processing and predictive analysis, making individuals subject to decisions based on invisible technological processes (Khan & Alam, 2026). Similarly, automated decision-making may affect equality and due process where individuals receive decisions without meaningful explanations or effective opportunities to challenge algorithmic outcomes (Citron, 2008).

Digital platforms have also transformed constitutional debates by shifting significant power from governments to private technology companies. Social media platforms increasingly influence access to information, public debate, and political participation through algorithmic recommendation and content moderation systems. These private actors perform functions that directly affect democratic communication and individual rights, raising questions regarding accountability, transparency, and the constitutional responsibilities of technology companies (De Gregorio, 2022). Therefore, contemporary constitutional analysis must consider not only traditional state power, but also technological power exercised through algorithms, platforms, and digital infrastructures.

In Pakistan, these challenges are particularly significant because the country is undergoing rapid digital transformation while its legal and institutional frameworks continue to develop. Government initiatives such as the Digital Pakistan Policy and emerging AI policy discussions demonstrate increasing recognition of technological innovation; however, legal preparedness and institutional capacity remain limited. Existing research indicates that Pakistan has developed important digital infrastructure, including identity management systems through NADRA, but lacks comprehensive mechanisms addressing algorithmic accountability, transparency, and responsible AI governance (Sarfraz & Fatima, 2024). Furthermore, existing legal instruments such as the Prevention of Electronic Crimes Act (PECA) 2016 primarily address conventional cybercrime and do not comprehensively regulate algorithmic decision-making, automated systems, or AI-related harms (Khan & Alam, 2026).

Traditional constitutional frameworks were primarily developed to regulate and limit governmental authority and protect individuals from state interference. However, the emergence of AI and digital governance has created new forms of power that operate beyond conventional constitutional boundaries. Algorithms, digital platforms, and technology companies increasingly influence decisions that affect individuals' rights, yet these systems often operate through complex technical processes that lack transparency and democratic oversight.

The central research problem is that existing constitutional and legal frameworks may not provide sufficient protection against harms generated by AI-driven governance. Automated decision-making systems may create challenges relating to accountability, explainability, equality, and access to remedies because individuals affected by algorithmic decisions may not understand how decisions were produced or who is responsible for potential harms (Yeung, 2018).

Pakistan faces additional challenges because constitutional protections were developed before the emergence of large-scale data processing and artificial intelligence. Although the Constitution of Pakistan provides important protections, including dignity and privacy under Article 14, fair trial, and due process under Article 10A, and freedom of expression under Article 19, these provisions require reinterpretation within contemporary digital environments (Khan & Alam, 2026). The absence of a comprehensive data protection framework and dedicated AI governance mechanism creates uncertainty regarding how constitutional rights should be protected in algorithmic societies.

Concept of Digital Constitutionalism

Digital constitutionalism refers to the process through which constitutional principles, values, and rights protections are adapted to address challenges created by digital technologies. Unlike traditional constitutionalism, which primarily focuses on restricting government power, digital constitutionalism recognizes that power in modern societies is also exercised through private technological infrastructures, algorithms, online platforms, and data-processing systems (De Gregorio, 2022).

At its core, digital constitutionalism seeks to ensure that technological development remains compatible with fundamental rights, democratic principles, and the rule of law. It provides a normative framework for regulating both public and private actors involved in digital governance by requiring accountability, transparency, human oversight, and protection of individual freedoms. The concept therefore extends constitutional reasoning into digital spaces where decisions affecting citizens may increasingly be produced through automated systems rather than traditional human authorities.

A key principle of digital constitutionalism is accountability. Since AI systems can influence decisions relating to employment, welfare, justice, and access to services, mechanisms must exist to identify responsibility for algorithmic outcomes. Transparency is equally important because individuals require meaningful information about how automated decisions are generated and how they may challenge unfair outcomes. Furthermore, digital constitutionalism emphasizes human rights protection, particularly privacy, equality, freedom of expression, and procedural fairness. International AI governance frameworks, including OECD AI Principles and UNESCO AI Ethics recommendations, similarly highlight transparency, accountability, human oversight, and human rights as essential elements of responsible AI governance (OECD, 2019; UNESCO, 2021).

Therefore, digital constitutionalism provides a bridge between technological innovation and constitutional democracy. Rather than restricting technological progress, it seeks to ensure that AI development occurs within a rights-based framework that preserves democratic accountability.

This article examines how digital constitutionalism can provide a framework for regulating artificial intelligence governance while protecting fundamental rights in Pakistan and the United Kingdom. Through comparative legal analysis, the research explores how constitutional principles can respond to emerging technological challenges and identifies possible lessons for strengthening Pakistan's AI governance framework.

Literature Review

The emergence of artificial intelligence (AI), algorithmic decision-making, and digital platforms has challenged the traditional understanding of constitutionalism. Classical constitutional theory was primarily concerned with limiting state authority through separation of powers, legality, and protection of individual rights. However, contemporary digital environments have transformed the nature of power by introducing new actors, including technology companies, online platforms, and algorithmic systems, that increasingly influence individual rights and democratic processes. As a result, scholars argue that constitutional thinking must expand beyond regulating governmental authority and address technological forms of power operating within digital societies (Celeste, 2019; De Gregorio, 2022).

Digital constitutionalism has emerged as a theoretical response to these developments. Celeste (2019) conceptualizes digital constitutionalism as a framework through which constitutional values are extended into digital environments. Rather than replacing traditional constitutionalism, it represents an adaptation of constitutional principles to new technological conditions. The central concern is that digital technologies create forms of power that may affect fundamental rights without fitting within traditional constitutional categories. Algorithms determine visibility of information, automated systems influence access to opportunities, and platforms establish rules governing online participation. Therefore, digital constitutionalism seeks to ensure that technological governance remains consistent with principles of human dignity, accountability, transparency, and the rule of law.

De Gregorio (2022) further develops this argument by highlighting the constitutional significance of digital platforms. According to this perspective, platforms increasingly perform functions that resemble public governance because they regulate access to information, control online communication, and influence democratic participation. This creates a constitutional challenge because private companies exercise significant social power without possessing the democratic legitimacy traditionally associated with public institutions. The literature therefore identifies a shift from constitutionalism concerned only with state power towards a broader model capable of regulating both governmental and private technological authority.

However, scholars disagree regarding the extent to which private digital actors can or should be understood through constitutional concepts. Iglesias Keller and Pereira (2025) critically argue that applying constitutional terminology to platform

governance creates theoretical difficulties because private companies cannot fully replicate constitutional institutions. Unlike governments, technology companies are not directly accountable through democratic processes, and their internal rules are often shaped by commercial interests rather than public values. This criticism highlights a fundamental tension within digital constitutionalism: while private platforms require accountability, excessive reliance on private governance mechanisms may weaken rather than strengthen democratic control.

Pollicino similarly identifies the constitutional challenges created by private digital power. The increasing influence of platforms over speech, information access, and social participation creates a situation where private entities perform functions with public consequences. However, regulating these actors requires careful consideration because traditional constitutional mechanisms were developed primarily to control state power rather than private technological infrastructures.

The literature therefore demonstrates that digital constitutionalism is not simply an extension of technology regulation. Instead, it represents a broader constitutional debate regarding how power should be controlled in societies where information, algorithms, and digital infrastructures shape individual experiences. The concept provides an important theoretical foundation for AI governance because artificial intelligence represents one of the strongest examples of technological power capable of affecting fundamental rights.

Digital constitutionalism is founded on the idea that constitutional principles must remain effective despite changes in the technological environment. The literature identifies several interconnected principles, including protection of fundamental rights, accountability of digital actors, transparency of technological systems, and preservation of democratic governance.

One of the most significant contributions of digital constitutionalism literature is the recognition that privacy has evolved from a traditional protection against physical intrusion into a broader right concerning informational autonomy. De Hert and Cocito (2024) argue that data protection has become an essential constitutional safeguard because modern societies increasingly depend upon the collection, processing, and exchange of personal information. Data protection principles provide individuals with mechanisms to control information flows and create accountability obligations for organizations handling personal data.

This argument is particularly relevant to AI governance because artificial intelligence systems depend upon extensive datasets. Unlike conventional decision-making processes, AI systems can generate predictions and classifications based on information that individuals may not know has been collected or analyzed. Therefore, privacy concerns in AI environments are not limited to unauthorized access but also include questions regarding inference, profiling, and automated decision-making.

Papakonstantinou further argues that digital transformation has created a new relationship between citizens, states, and information infrastructures. Governments increasingly operate as digital platforms, collecting and processing large amounts of personal information to provide public services. While digital government can improve efficiency and accessibility, it also creates risks concerning surveillance, transparency, and accountability. This demonstrates that digital constitutionalism must address not only private technology companies but also state use of digital systems.

The principle of accountability represents another central element of digital constitutionalism. Traditional legal systems generally assign responsibility to identifiable decision-makers. However, AI systems complicate responsibility because decisions may result from complex interactions between datasets, algorithms, developers, and organizations. Yeung (2018) argues that algorithmic regulation creates challenges because automated systems can influence behavior while operating with limited transparency. Therefore, accountability mechanisms are necessary to ensure that technological systems remain subject to legal oversight.

Transparency is closely connected with accountability. Individuals affected by algorithmic decisions require meaningful information regarding how decisions are produced and whether they can challenge incorrect outcomes. Without transparency, AI governance risks creating a situation where individuals are governed by systems they cannot understand or contest.

Nevertheless, the literature also identifies limitations within digital constitutionalism. While the concept successfully highlights emerging technological challenges, some scholars argue that it remains more normative than operational. Digital constitutionalism provides principles for governing digital power but does not always provide specific institutional arrangements or enforcement mechanisms. Therefore, translating digital constitutional values into practical AI governance frameworks remains a continuing challenge.

The literature on AI governance demonstrates that artificial intelligence has moved beyond experimental technology and has become increasingly embedded within administrative, economic, and social systems. AI applications are now used in areas

including financial decision-making, healthcare, employment recruitment, policing, welfare administration, and legal services. These developments provide opportunities for efficiency and improved decision-making; however, they also create significant legal and constitutional concerns.

Wirtz et al. (2019) argue that AI adoption within public administration has the potential to improve government efficiency, service delivery, and policy analysis. However, they emphasize that AI implementation requires careful governance because automated systems may create challenges relating to transparency, accountability, and ethical responsibility. Similarly, Zuiderwijk et al. (2021) highlight that AI-driven public sector innovation requires institutional capacity and regulatory frameworks capable of addressing risks associated with automated decision-making.

The legal sector represents an important example of both the opportunities and risks associated with AI governance. Afzal and Ghawaas (2025) examine AI adoption within Pakistan's civil justice system and argue that technologies such as online dispute resolution, legal information systems, and document automation may improve access to justice. However, they emphasize that technological efficiency must remain subject to constitutional safeguards, particularly fair trial rights, equality, and procedural fairness.

The literature identifies algorithmic opacity as one of the most significant challenges associated with AI governance. Unlike traditional administrative decisions where reasoning may be explained by human decision-makers, AI systems often operate through complex computational processes that are difficult to interpret. This creates concerns regarding whether individuals can effectively challenge decisions affecting their rights.

Citron (2008) describes this challenge as technological due process, arguing that automated systems must preserve procedural protections traditionally associated with legal decision-making. The concern is not simply whether AI systems produce accurate outcomes but whether individuals have access to explanation, review, and correction mechanisms.

Algorithmic power therefore creates a constitutional challenge because it changes the nature of decision-making authority. Decisions previously made by identifiable individuals may now be influenced or determined by computational systems. Digital constitutionalism provides a framework for addressing this challenge by requiring that AI systems remain accountable to human rights principles.

A major concern within the literature on artificial intelligence governance is the relationship between algorithmic decision-making and equality rights. Although AI systems are frequently presented as objective and neutral technologies, scholars argue that algorithms may reproduce existing social inequalities because they are developed using historical datasets, institutional practices, and human-defined assumptions. Consequently, algorithmic systems may transform existing forms of discrimination into automated decision-making processes that appear technically legitimate but produce unequal outcomes.

O'Neil (2016) argues that mathematical models are not inherently impartial because they reflect the values, assumptions, and limitations of their creators. When deployed in high-impact areas such as employment, financial services, education, and criminal justice, algorithmic systems can disadvantage individuals whose characteristics are poorly represented within training datasets. Similarly, Noble (2018) demonstrates that algorithmic systems can reproduce social hierarchies by embedding existing cultural and institutional biases into technological infrastructures.

The literature on algorithmic injustice is particularly relevant to Pakistan because existing social inequalities may influence the operation of AI systems. Lodhi et al. (2026) examine algorithmic injustice within Pakistan's emerging AI governance landscape and argue that automated decision-making systems may create significant risks for women and marginalized communities. Their analysis highlights that AI systems trained on unequal social data may interpret existing discrimination as legitimate predictive information rather than recognizing it as a reflection of structural inequality. Therefore, algorithmic decision-making may reinforce disadvantages in areas such as employment, financial access, education, and public services.

This concern is intensified in Pakistan because digital transformation is occurring within a social environment where unequal access to technology already exists. Kalsoom (2026) argues that AI-driven digital environments create specific challenges for women's rights, particularly regarding online participation, synthetic media, automated harassment, and algorithmic control of visibility. The study highlights that AI governance must consider not only technological efficiency but also the social consequences of digital systems on participation and equality.

However, existing literature on algorithmic bias has certain limitations. Much of the scholarship focuses on identifying discriminatory outcomes rather than developing constitutional mechanisms capable of preventing such harms. While identifying bias is important, digital constitutionalism requires a broader approach that connects algorithmic fairness with legal accountability, transparency, and enforceable rights. Therefore, algorithmic equality cannot be achieved merely through

technical improvements to AI systems; it requires constitutional and institutional safeguards ensuring that affected individuals have meaningful remedies.

The concept of digital constitutionalism contributes to this debate by reframing algorithmic bias as a constitutional issue rather than merely a technological problem. If AI systems influence access to employment, justice, welfare, or public participation, then discriminatory outcomes raise fundamental questions concerning equality, dignity, and rule of law. Consequently, AI governance requires mechanisms capable of ensuring that technological systems operate consistently with constitutional principles.

Privacy represents one of the most significant areas where artificial intelligence challenges existing constitutional frameworks. Traditional privacy law was primarily designed to address visible forms of interference, such as physical intrusion, unauthorised access, or disclosure of confidential information. However, AI has transformed the nature of privacy risks because modern surveillance operates through continuous collection, processing, and inference from personal data.

Khan and Alam (2026) argue that artificial intelligence has fundamentally changed the meaning of privacy in Pakistan because modern surveillance no longer depends exclusively upon direct observation. Instead, AI-enabled systems can collect and analyse identity information, biometric data, location records, financial information, health data, and behavioural patterns. Individuals may therefore experience privacy harms even when they are not directly monitored because algorithmic systems can generate predictions and classifications from accumulated datasets.

Pakistan's constitutional framework provides an important foundation for privacy protection. Article 14 of the Constitution guarantees the dignity of individuals and privacy of the home. However, Khan and Alam (2026) argue that although constitutional principles provide normative protection, existing legal mechanisms remain insufficient for addressing AI-specific privacy challenges. The current framework regulates forms of digital harm but does not provide comprehensive rights relating to algorithmic profiling, automated decision-making, data portability, explanation of AI decisions, or compensation for misuse of personal information.

The Supreme Court of Pakistan has played an important role in developing privacy jurisprudence. In *Mohtarma Benazir Bhutto v President of Pakistan*, the Court examined telephone interception and surveillance practices, recognising that privacy protection extends beyond physical spaces. The Court's reasoning demonstrated that constitutional privacy must adapt to technological developments because communication and personal information can be violated through modern forms of surveillance. This approach aligns with digital constitutionalism because it recognises that constitutional rights must remain effective despite technological transformation.

However, the literature identifies a significant gap between constitutional recognition and practical protection. Khan and Alam (2026) argue that Pakistan's existing framework consists of fragmented protections through constitutional rights, cybercrime legislation, surveillance laws, and general civil remedies. While these mechanisms may address individual violations, they do not establish a comprehensive horizontal privacy regime applicable to both public authorities and private data controllers.

The absence of comprehensive data protection legislation creates challenges for AI governance because artificial intelligence depends upon extensive personal data processing. Without clear obligations regarding lawful processing, transparency, accountability, and individual control over information, AI systems may operate without adequate constitutional safeguards.

Digital Constitutionalism in Pakistan

The constitutional framework of Pakistan provides a significant normative foundation for digital constitutionalism, despite being developed before the emergence of artificial intelligence and algorithmic governance. The central challenge is not the absence of constitutional values but the difficulty of translating traditional rights into technological environments where power is exercised through data collection, automated decisions, and digital infrastructure.

Digital constitutionalism requires constitutional rights to be interpreted dynamically because AI systems create forms of interference that differ from traditional exercises of state authority. Unlike conventional surveillance, algorithmic governance operates through continuous collection, processing, and prediction of personal information. Individuals may experience rights violations not through direct government action but through decisions generated by public authorities, private platforms, or automated systems.

Pakistan's constitutional protections therefore provide the starting point for regulating AI, but constitutional interpretation alone cannot substitute for comprehensive legislative safeguards.

Article 9 provides that no person shall be deprived of life or liberty except in accordance with law. Traditionally, this provision has been associated with physical liberty; however, contemporary constitutional interpretation increasingly recognizes that liberty includes broader aspects of personal autonomy and decision-making.

AI governance creates new challenges for Article 9 because algorithmic systems may influence decisions affecting employment opportunities, access to financial services, welfare benefits, and criminal justice outcomes. When individuals are subjected to automated decisions without explanation or meaningful review, the constitutional principle of liberty becomes weakened.

The problem is not merely technological accuracy but legal accountability. Even technically accurate systems may create constitutional concerns if affected individuals cannot understand, challenge, or correct decisions. Therefore, Article 9 should be interpreted alongside principles of transparency and procedural fairness.

Article 10A guarantees the right to fair trial and due process. Within the context of AI governance, this provision becomes particularly important because automated decision-making can affect individuals without traditional procedural safeguards.

Algorithmic systems often operate through complex models that are difficult for individuals to understand. This creates what Citron (2008) describes as the problem of technological due process, where individuals are subject to decisions made by automated systems without adequate explanation or opportunity for challenge.

The constitutional importance of Article 10A is therefore not limited to judicial proceedings. It provides a broader principle requiring fairness whenever state decisions significantly affect individuals. AI systems used by public authorities should therefore incorporate meaningful human oversight, explanation mechanisms, and review procedures.

Without these safeguards, algorithmic governance risks replacing accountable decision-making with opaque technological processes.

Article 14 represents the strongest constitutional foundation for digital privacy protection in Pakistan. The provision states that “the dignity of man and, subject to law, the privacy of home, shall be inviolable.” Although the constitutional language refers specifically to the privacy of the home, Pakistani jurisprudence has adopted an expansive interpretation.

The Supreme Court’s decision in *Mohtarma Benazir Bhutto v President of Pakistan* remains central because it recognized that privacy cannot be restricted to a physical location. Drawing upon comparative reasoning from *Katz v United States*, the Court accepted that privacy depends upon reasonable expectations rather than geographical boundaries. Therefore, communication, personal information, and behavioral data may fall within constitutional protection.

This reasoning is highly relevant in the AI era because modern surveillance operates through biometric databases, digital identities, online behavior tracking, and predictive analytics. Khan and Alam (2026) argue that existing Pakistani laws address specific forms of digital intrusion but fail to establish comprehensive protections for algorithmic profiling, automated decision-making, and data misuse.

However, a critical limitation remains. Article 14 provides constitutional recognition but does not establish detailed obligations for data controllers. Unlike the UK GDPR, Pakistan lacks comprehensive statutory rights relating to data access, correction, deletion, algorithmic explanation, and automated decision-making safeguards.

Article 19 protects freedom of speech and expression, subject to constitutional restrictions. In digital societies, freedom of expression increasingly depends upon access to online platforms and communication networks.

Artificial intelligence creates new challenges because expression may be affected through automated content moderation, predictive monitoring, and algorithmic visibility systems. Furthermore, state-controlled restrictions on digital access raise constitutional concerns.

The jurisprudence concerning internet shutdowns demonstrates this challenge. In *CM Pak Limited v Pakistan Telecommunications Authority*, the Islamabad High Court held that government-directed network suspensions must operate within legal authority and cannot impose disproportionate restrictions. The judgment recognized that communication restrictions affect fundamental rights, including access to information and expression.

Therefore, digital constitutionalism requires that restrictions on digital communication satisfy legality, necessity, and proportionality principles.

Article 19A provides citizens with the right to access information held by public bodies. In the context of AI governance, this right has increasing importance because transparency regarding automated systems is essential for accountability.

The Supreme Court's interpretation of Article 19A has strengthened the principle that access to information is a constitutional entitlement rather than administrative discretion.

Applied to AI governance, Article 19A supports demands for greater transparency regarding government algorithms, automated decision-making processes, and digital systems affecting citizens.

Pakistan's current digital governance framework provides partial protection against technological harms but remains fragmented. The Prevention of Electronic Crimes Act 2016 represents the principal legislation addressing cyber-related offences, including unauthorized access, identity misuse, and unlawful interception.

However, PECA was developed primarily as a cybercrime statute rather than an AI governance framework. Consequently, it does not adequately address emerging issues such as algorithmic bias, automated discrimination, explainability requirements, or accountability of private technology companies.

The distinction is important because AI-related harms often occur through lawful data collection followed by harmful processing. Traditional cybercrime legislation focuses mainly on unlawful access, whereas AI governance requires regulation of legitimate but potentially harmful uses of data.

Although Pakistan possesses constitutional foundations for digital rights protection, significant gaps remain between constitutional principles and technological realities.

The first limitation is the absence of a comprehensive AI governance framework. Existing laws regulate specific digital harms but do not establish general principles governing AI development, deployment, auditing, and accountability.

Second, Pakistan lacks strong algorithmic accountability mechanisms. Automated decisions affecting citizens require transparency obligations, impact assessments, and independent oversight. Without these mechanisms, individuals may be unable to challenge discriminatory or erroneous outcomes.

Third, data protection remains insufficient. AI systems depend upon extensive personal information, yet fragmented regulation creates risks of surveillance and misuse. Amnesty International's analysis of surveillance and censorship practices in Pakistan highlights broader concerns regarding monitoring infrastructure, interception systems, and restrictions on digital communication.

Therefore, the challenge for Pakistan is not simply technological adoption but constitutional governance of technology. Digital constitutionalism provides a framework for ensuring that AI development remains compatible with dignity, privacy, equality, expression, and due process.

Digital Constitutionalism in the United Kingdom

Unlike Pakistan, where digital rights protection has largely developed through constitutional interpretation and judicial expansion of existing rights, the United Kingdom has approached digital constitutionalism through a combination of human rights legislation, data protection law, regulatory institutions, and technology-specific governance initiatives. Although the UK does not possess a single written constitutional document, constitutional principles are embedded through statutes, judicial review, common law protections, and international human rights obligations. In the digital context, the Human Rights Act 1998 (HRA) provides the primary rights-based framework through which technological interference with fundamental freedoms is assessed.

The Human Rights Act incorporates rights contained within the European Convention on Human Rights (ECHR) into domestic law. This framework has become increasingly significant as artificial intelligence, automated decision-making, and digital surveillance create new forms of interference with individual rights. However, the UK approach demonstrates that constitutional protection in the digital age requires more than formal recognition of rights; it requires institutional mechanisms capable of ensuring that public and private actors exercise technological power responsibly.

Article 8 of the ECHR, protecting the right to respect for private and family life, home, and correspondence, represents the central legal basis for digital privacy protection in the UK. The provision has been interpreted broadly by the European Court of Human Rights and UK courts to include protection against modern forms of surveillance, data collection, and state monitoring. Unlike traditional privacy concepts focused on physical intrusion, Article 8 has developed into a protection of personal autonomy and informational privacy.

This broader interpretation is particularly relevant to artificial intelligence because AI systems operate through extensive processing of personal information. Automated profiling, biometric recognition, predictive analytics, and behavioral

monitoring may affect individuals without direct physical interference. Therefore, Article 8 provides a constitutional basis for questioning whether data-driven systems operate proportionately and whether adequate safeguards exist against misuse.

The importance of Article 8 has been demonstrated through surveillance jurisprudence. In *R (Bridges) v Chief Constable of South Wales Police* [2020], the Court of Appeal examined the use of live facial recognition technology by police authorities. Although the court did not prohibit the technology entirely, it emphasized that deployment of AI-based surveillance must comply with legal requirements, including adequate safeguards and clear criteria governing its use. The decision illustrates a central principle of digital constitutionalism: technological capability does not remove the obligation to respect fundamental rights.

Article 10 ECHR, protecting freedom of expression, is also increasingly important in digital environments. Online platforms have become central spaces for political participation, public debate, and information exchange. However, algorithmic recommendation systems, automated content moderation, and platform governance decisions influence what information individuals see and how speech circulates. De Gregorio (2021) argues that digital platforms increasingly perform quasi-constitutional functions because their private rules influence democratic participation and freedom of expression.

The challenge for digital constitutionalism is therefore that expression rights are no longer affected only by state censorship. Private technology companies increasingly control communication infrastructures and may restrict visibility, access, or distribution of speech through automated systems. The UK and European regulatory approach attempt to address this issue by imposing greater transparency and accountability obligations on digital platforms.

Article 6 ECHR, which protects the right to a fair hearing, provides another important foundation for regulating automated decision-making. As AI systems become increasingly involved in administrative decisions, questions arise regarding whether individuals receive adequate explanations, whether decisions can be challenged effectively, and whether human review remains available. Citron (2008) describes this issue as technological due process, arguing that automated systems must preserve procedural fairness rather than replacing accountable decision-making with opaque computational processes.

However, the UK framework also faces limitations. Human rights legislation provides important principles but does not independently regulate every aspect of AI governance. Rights-based review often occurs after potential harm has occurred, whereas AI regulation requires preventative mechanisms such as impact assessments, auditing, and transparency obligations. Therefore, the UK approach demonstrates that constitutional rights must be supported by specialized regulatory structures.

Data protection represents the most developed element of the UK's digital constitutionalism framework. The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) establish comprehensive rules governing the collection, processing, storage, and use of personal data. These laws recognize that information control has become central to individual autonomy in digital societies.

The UK GDPR is based upon several principles including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, security, and accountability. These principles are particularly significant for AI governance because artificial intelligence systems depend upon large-scale data processing. By requiring organizations to justify data processing activities and maintain accountability, data protection law creates important constraints on technological power.

A major contribution of the UK GDPR is its recognition of individual rights in relation to automated decision-making. Article 22 provides safeguards where individuals are subject to decisions based solely on automated processing that produce legal or similarly significant effects. Individuals may have rights relating to human intervention, explanation, and contesting decisions. These protections directly address concerns surrounding algorithmic opacity and lack of procedural fairness.

However, scholars have questioned whether existing data protection rules are sufficient for advanced AI systems. Wachter, Mittelstadt, and Floridi (2017) argue that the right to explanation remains uncertain because legal frameworks often do not clearly define the level of information organizations must provide regarding algorithmic decisions. Similarly, Edwards and Veale (2017) suggest that traditional data protection mechanisms may struggle with complex machine-learning systems because many AI harms arise not from individual data points but from broader patterns and inferences.

Therefore, although the UK GDPR represents a significant development in digital rights protection, it should not be viewed as a complete solution to AI governance challenges. Data protection primarily regulates information processing, whereas AI governance also requires attention to discrimination, accountability, safety, and institutional responsibility.

The Data Protection Act 2018 complements the UK GDPR by providing domestic legal mechanisms and establishing the role of the Information Commissioner's Office (ICO) as an independent regulatory authority. The ICO has developed guidance on AI

and data protection, emphasizing transparency, fairness, accountability, and human oversight. This institutional approach demonstrates an important feature of digital constitutionalism: rights require enforcement institutions capable of translating principles into practical governance.

The UK's AI governance approach differs from the European Union's more centralized regulatory model. Rather than introducing a single comprehensive AI statute, the UK has adopted a principles-based and risk-oriented approach. The government's AI White Paper proposed a framework based on five principles: safety, transparency, fairness, accountability, and contestability (Department for Science, Innovation and Technology, 2023).

This approach reflects the UK's attempt to balance technological innovation with rights protection. Rather than imposing broad restrictions on AI development, the framework seeks to ensure that AI systems are deployed responsibly according to the risks they create.

Transparency represents a central element of this approach. AI systems that affect individuals must provide sufficient information regarding their operation, purpose, and limitations. Without transparency, individuals cannot meaningfully challenge automated decisions or identify discriminatory outcomes.

Accountability is equally important because responsibility for AI decisions cannot be transferred to technology itself. Organizations deploying AI systems must remain responsible for outcomes generated through those systems. This principle challenges the argument that algorithmic decisions are neutral or inevitable.

Institutional oversight is another important component of the UK approach. Regulatory bodies such as the ICO, Competition and Markets Authority, and Equality and Human Rights Commission contribute to AI governance within their respective areas. However, the fragmented nature of this model has generated debate regarding whether existing institutions possess sufficient powers and coordination mechanisms to regulate rapidly evolving AI technologies.

Overall, the UK experience demonstrates that effective digital constitutionalism requires integration between constitutional rights, regulatory institutions, and technological governance mechanisms. Nevertheless, Pakistan's different constitutional structure and institutional capacity mean that UK approaches must be adapted rather than directly replicated.

Comparative Analysis: Pakistan and United Kingdom

Despite significant differences between Pakistan and the United Kingdom, both jurisdictions recognize that digital technologies create challenges requiring a balance between innovation and fundamental rights protection. In both systems, privacy has become a central constitutional concern because AI systems depend upon extensive collection and analysis of personal information.

Pakistan's Article 14 protection of dignity and privacy and the UK's Article 8 ECHR protection reflect a shared recognition that individuals require protection against unjustified interference with personal autonomy. However, the mechanisms through which these rights are protected differ significantly.

Both jurisdictions also recognize the importance of freedom of expression in digital environments. Internet platforms have transformed communication, but they have also created challenges concerning surveillance, censorship, and algorithmic control of information. Consequently, both countries face questions regarding how democratic values can be preserved when communication increasingly occurs through privately controlled digital infrastructures.

Furthermore, both Pakistan and the UK acknowledge the need for AI accountability. Automated decision-making creates similar concerns across jurisdictions, including lack of transparency, potential discrimination, and difficulties challenging algorithmic outcomes.

The major difference between Pakistan and the UK concerns institutional maturity and regulatory development. Pakistan's approach remains primarily constitutional and judicial, whereas the UK has developed a broader regulatory ecosystem supported by legislation and independent institutions.

Pakistan possesses strong constitutional principles but lacks comprehensive AI-specific legislation. Existing laws such as PECA provide protection against certain cyber harms but do not establish detailed requirements for algorithmic transparency, auditing, or automated decision-making safeguards. Consequently, protection often depends upon judicial interpretation after disputes arise.

The UK, by contrast, has developed more comprehensive mechanisms through the UK GDPR, Data Protection Act 2018, Human Rights Act 1998, and regulatory guidance. These mechanisms provide clearer obligations for organizations processing

personal data and deploying automated systems. Institutional oversight also represents a significant difference. Pakistan's digital governance institutions remain developing, whereas the UK benefits from established regulatory bodies such as the ICO. However, the UK system also faces challenges because AI governance responsibilities are distributed across multiple institutions, creating questions regarding coordination and enforcement.

Digital rights jurisprudence similarly demonstrates different levels of development. Pakistani courts have played an important role in expanding constitutional protections, particularly regarding privacy and internet access. UK courts operate within a more established human rights framework where digital rights are integrated through statutory interpretation and regulatory review.

The UK experience provides several important lessons for Pakistan, although these should be adapted according to Pakistan's constitutional and institutional context.

First, Pakistan requires a stronger personal data protection framework. Constitutional recognition of privacy is important but insufficient without detailed statutory rights relating to data access, correction, deletion, and automated processing.

Second, Pakistan should introduce stronger AI transparency obligations. Individuals affected by AI-driven decisions should have meaningful opportunities to understand and challenge outcomes.

Third, independent regulatory oversight is essential. A dedicated institution responsible for AI governance and data protection could improve accountability and ensure consistent enforcement.

Fourth, Pakistan should consider algorithmic impact assessments for high-risk AI systems. These assessments could identify potential discrimination, privacy risks, and procedural concerns before deployment.

Finally, digital rights protection should remain central to AI development. Technological innovation should not be viewed as separate from constitutional values. Instead, AI governance should ensure that innovation operates within principles of dignity, equality, accountability, and rule of law.

Proposed Digital Constitutionalism Model for Pakistan

A suitable digital constitutionalism model for Pakistan should combine constitutional rights protection with institutional and regulatory mechanisms capable of addressing AI-specific challenges. Rather than adopting foreign frameworks unchanged, Pakistan requires a context-sensitive approach reflecting its constitutional structure, technological development, and governance realities.

The first pillar should be rights-based AI governance. AI systems must operate consistently with constitutional protections of privacy, equality, dignity, and fairness. This requires recognizing digital rights as extensions of existing constitutional guarantees rather than entirely new categories of rights.

The second pillar should be algorithmic accountability. Pakistan should introduce requirements for explainability, human oversight, and independent auditing of high-impact AI systems. Automated decisions affecting employment, welfare, justice, or access to essential services should not occur without meaningful review mechanisms.

The third pillar should involve institutional reform. Pakistan requires stronger governance institutions capable of supervising AI deployment. A dedicated data protection authority and AI regulatory body could provide oversight, while courts should retain the ability to review AI-related decisions affecting fundamental rights.

The fourth pillar should focus on balancing innovation with constitutional limits. Effective AI governance should not prevent technological development but should ensure that innovation occurs responsibly. A rights-based approach can increase public trust by ensuring that AI systems operate transparently and fairly.

Artificial intelligence has transformed the relationship between technology, governance, and constitutional rights. Traditional constitutional frameworks were designed primarily to control visible exercises of state power; however, AI introduces new forms of power exercised through algorithms, data infrastructures, and digital platforms. These developments require constitutional principles to evolve to protect individuals within increasingly digital societies.

Digital constitutionalism provides an important theoretical framework because it extends constitutional values of accountability, transparency, dignity, and human rights protection into technological environments. Both Pakistan and the United Kingdom demonstrate that privacy, expression, equality, and due process remain central concerns in AI governance.

The UK experience illustrates the importance of combining human rights protection with detailed regulatory mechanisms, including data protection law, independent oversight, and transparency requirements. However, Pakistan cannot simply replicate the UK model because differences exist in constitutional structures, institutional capacity, and technological development.

Pakistan already possesses constitutional foundations capable of supporting digital rights protection, particularly through Articles 9, 10A, 14, 19, and 19A. Judicial developments demonstrate that these provisions can adapt to technological challenges. Nevertheless, constitutional interpretation alone cannot address all AI governance challenges. Comprehensive data protection legislation, algorithmic accountability mechanisms, and institutional reforms are required.

A locally adapted digital constitutionalism framework would allow Pakistan to pursue technological innovation while ensuring that artificial intelligence develops within constitutional boundaries. The future of AI governance should therefore not be determined only by technological capability but by the extent to which technology remains accountable to human rights, democratic values, and the rule of law.

References

Legislation

Constitution of Pakistan. (1973). *The Constitution of the Islamic Republic of Pakistan*.

Data Protection Act 2018 (UK).

Human Rights Act 1998 (UK).

Regulation (EU) 2016/679. (2016). *General Data Protection Regulation (GDPR)*.

Prevention of Electronic Crimes Act 2016 (Pakistan).

Cases

Mohtarma Benazir Bhutto v President of Pakistan, PLD 1988 SC 416.

CM Pak Limited v Pakistan Telecommunications Authority, W.P. No. 1755/2018 (Islamabad High Court).

PTA v CM Pak Limited, Civil Petition No. 1548-L/2019 (Supreme Court of Pakistan).

Katz v United States, 389 U.S. 347 (1967).

Secondary Sources

Afzal, M., & Ghawaas, M. (2025). Artificial intelligence and access to justice in Pakistan: Opportunities, challenges, and constitutional implications. *[Journal/Publisher details as provided in source document]*.

Amnesty International. (2025). *Pakistan: Surveillance, censorship, and digital rights concerns in the age of technology*. Amnesty International.

Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology*, 33(1), 76–99. <https://doi.org/10.1080/13600869.2019.1562609>

Celeste, E. (2023). *Digital constitutionalism: The role of Internet bills of rights*. Routledge.

Celeste, E., & De Gregorio, G. (2022). Digital humanism: The constitutional message of the GDPR. *Global Privacy Law Review*, 3(1), 1–15.

Celeste, E., & De Gregorio, G. (2023). Towards a right to digital education? Constitutional challenges of edtech. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 14(2), 234–250.

Citron, D. K. (2008). Technological due process. *Washington University Law Review*, 85(6), 1249–1313.

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, 19(1), 41–70.

De Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing fundamental rights and democracy in the algorithmic society*. Cambridge University Press. <https://doi.org/10.1017/9781009071215>

- De Gregorio, G. (2022). Digital constitutionalism across the Atlantic. *Global Constitutionalism*, 11(2), 297–324. <https://doi.org/10.1017/S2045381722000016>
- De Gregorio, G., & Dunn, P. (2022). The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review*, 59(2), 473–500.
- De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, 30(1), 68–87. <https://doi.org/10.1093/ijlit/eaac004>
- De Gregorio, G., & Stremlau, N. (2021). Platform governance at the periphery: Moderation, shutdowns, and intervention. In J. Bayer, B. Holznagel, P. Korpisaari, & L. Woods (Eds.), *Perspectives on platform regulation: Concepts and models of social media governance across the globe* (pp. 433–450). Nomos.
- De Gregorio, G., Pollicino, O., & Valcke, P. (Eds.). (2024). *The Oxford handbook of digital constitutionalism*. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780198877820.001.0001>
- De Hert, P., & Cocito, C. (2024). The added value of data protection within the framework of digital constitutionalism in Europe. In G. De Gregorio, O. Pollicino, & P. Valcke (Eds.), *The Oxford handbook of digital constitutionalism*. Oxford University Press.
- Department for Science, Innovation and Technology. (2023). *A pro-innovation approach to AI regulation*. UK Government.
- Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a “right to explanation” is probably not the remedy you are looking for. *Duke Law & Technology Review*, 16, 18–84.
- Haider, M., & Haider, S. (2026). Artificial intelligence governance in Pakistan: Regulatory challenges and comparative perspectives. [Journal details as provided in source document].
- Iglesias Keller, C., & Pereira, J. R. G. (2025). Digital constitutionalism as an online speech governance framework: A critical approach. [Publication details as provided in source document].
- Kalsoom, S. (2026). Gender-responsive artificial intelligence governance and women’s digital rights in Pakistan. [Journal details as provided in source document].
- Khan, M. Z., & Alam, F. (2026). The right to privacy in the age of artificial intelligence: Evaluating Pakistan’s civil law protections against algorithmic surveillance and data misuse. *Innovative Research Journal of Artificial Intelligence*, 4(1), 1–19. <https://doi.org/10.62497/irjai.239>
- Lodhi, N. H., Raza, M., & Saleem, H. (2026). Algorithmic injustice: Reconceptualizing legal framework for women rights in Pakistan’s emerging AI governance landscape. *The Critical Review of Social Sciences Studies*, 4(1), 4813–4834.
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.
- O’Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.
- Papakonstantinou, V. (2024). Digital constitutionalism and the evolution of information rights. In G. De Gregorio, O. Pollicino, & P. Valcke (Eds.), *The Oxford handbook of digital constitutionalism*. Oxford University Press.
- Pollicino, O., & De Gregorio, G. (2022). Constitutional democracy, platform powers and digital populism. *Constitutional Studies*, 8, 11–30.
- Sarfraz, S. B., & Fatima, S. (2024). Digital government readiness and legal preparedness for artificial intelligence adoption in Pakistan’s public sector. *Journal of Development and Social Sciences*, 5(4), 714–727.
- UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ixx005>
- 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.
- Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523.

Zuiderwijk, A., Chen, Y. C., & Salem, M. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38(3), 101577.



2026 by the authors; Journal of Kashmir Journal of Academic Research and Development. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).