JOURNAL OF CRIMINOLOGY AND CRIMINAL JUSTICE

Vol.1, No.1 2025 E-ISSN. 3137-0543. P-ISSN. 3137-0535 OPEN ACCESS

RESEARCH ARTICLE // DOUBLE-BLIND PEER REVIEWED

Digital Transformation and Administrative Law: *Reconstructing Legality, Discretion and Accountability in Digital Public Administration*

Muhammad Ahmed Maqbool[1*] ◆ **Bauryzhan Yessov**[2]

[1] LLM in International Business Law from Leeds Beckett University, United Kingdom. Email: ahmedmaqbool1215@gmail.com

ORCID https://orcid.org/ 0009-0005-0475-3186

[2] Political Science and International Relations, Nazarbayev University Graduate School of Public Policy (NU GSPP), Astana, Kazakhstan.

Email: bauyrzhan.yessov@nu.edu.kz

ABSTRACT

Digital transformation is changing not only how public services are delivered but also where administrative discretion, evidence and responsibility are located. Governments increasingly rely on interoperable databases, digital identity, automated eligibility systems, risk scoring, predictive analytics and artificial-intelligence tools. This article examines the resulting problem from an administrative-law perspective: to what extent does digital transformation require a reconstruction of traditional principles of legality, reason-giving, procedural fairness, accountability and judicial review? The study employs qualitative doctrinal and comparative legal analysis of primary legal instruments, judicial decisions, international standards and recent scholarship, with particular attention to the European Union and selected comparative developments, and applies the framework to Pakistan's emerging digital-governance architecture. It argues that digitalisation does not eliminate administrative discretion; it redistributes discretion across legislation, software, datasets, procurement decisions, vendors and frontline officials. This redistribution creates four connected legal problems: the legal authority for high-impact automation; the reconstruction of the administrative record and reasons when decisions are produced through socio-technical systems; accountability when public functions are outsourced; and equality and access where digital channels become conditions of public-service delivery. The article further argues that data protection, cybersecurity, procurement and digital inclusion should be treated as components of administrative accountability rather than as separate technical policy fields. The comparative analysis shows that the European Union provides an important but non-transplantable regulatory reference point, while Pakistan illustrates the sequencing challenge created by rapid digital public infrastructure development alongside an incomplete comprehensive data-protection framework. The article proposes a framework based on legally specific authorization for high-impact automation, meaningful human review, reconstructable digital administrative records, procurement safeguards, purpose limitation, coordinated oversight and equivalent non-digital access to essential public services.

01 ARTICLE HISTORY

Received 08-08-2025
Accepted 20-12-2025
Published 30-12-2025

02 KEYWORDS

Digital government; digital governance; administrative law; algorithmic decision-making; administrative discretion; rule of law; artificial intelligence; algorithmic

03 CORRESPONDING AUTHOR

Muhammad Ahmed Maqbool
ahmedmaqbool1215@gmail.com

CC BY-NC 4.0 © 2025 The Author(s). Published by JuriSocial Research Center Private Limited. This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International Licence (https://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.68740/jjccj12

1. Introduction

Public administration is being rebuilt on digital foundations. Ministries now operate through integrated identity systems, interoperable registries, workflow platforms, data lakes, and machine-learning tools that classify applicants, detect anomalies, allocate inspections, and, in some settings, generate first-draft administrative determinations. Citizens encounter the state not only at counters and in hearing rooms but through mobile applications, chatbots, notification systems, and automated eligibility engines. This shift is often described as modernization. In institutional terms, however, it is a transformation of the architecture of public power. Decision-making is being relocated from individual officers to socio-technical systems; records that once existed as paper files are becoming reusable data assets; and the boundary between public authority and private infrastructure is becoming more porous as governments procure cloud services, proprietary algorithms, and platform interfaces from commercial vendors (Dunleavy et al., 2006; Mergel et al., 2019; Giest & Roberge, 2025).

The promise is substantial. Digital systems can reduce processing times, expand access for remote populations, improve targeting of scarce resources, and generate evidence for policy evaluation. The United Nations E-Government Survey 2024 reports a marked rise in digital government maturity across Member States and a decline in the share of the world's population living in countries with lagging e-government development (United Nations Department of Economic and Social Affairs [UN DESA], 2024). The Organisation for Economic Co-operation and Development has likewise framed digital technologies and data as essential to public-sector performance, resilience, and trust, while cautioning that public confidence in governments' use of personal data and new technologies remains fragile (Organisation for Economic Co-operation and Development [OECD], 2020, 2025, 2026). These findings capture a dual reality: digital government is advancing, yet legitimacy has not automatically followed capability.

That dual reality is the point of departure for this article. Digital governance is not merely the digitization of existing procedures. It is a mode of governing in which data, code, and platforms become instruments of public authority. Once that occurs, legal and policy questions that were once secondary—how a form is stored, how a queue is managed, how a file is transferred—become constitutional questions in miniature. Who may collect which data, for what purpose, and for how long? When may an algorithm lawfully determine, or substantially determine, an individual's legal position? What does reasoned decision-making require when the operative reasoning is distributed across training data, model weights, vendor documentation, and a frontline officer's click? How should liability be allocated when harm arises from a composite system involving a ministry, a contractor, a cloud provider, and a model that no single official fully understands? How can the state remain inclusive when services migrate online while digital literacy, connectivity, language, disability access, and trust remain unevenly distributed?

The European Union's Artificial Intelligence Act establishes a risk-based framework and identifies specified AI uses in areas including access to essential public services, law enforcement and migration among categories that may be high-risk, subject to the Act's classification rules and annexes. The article therefore does not treat all public-sector AI as automatically high-risk; classification depends on the system, intended purpose and applicable provisions of Regulation (EU) 2024/1689.

The scholarly literature has tracked this movement from e-government to digital government and digital governance, emphasizing not only tools but also institutional redesign, citizen–state relations, and public value (Bannister & Connolly, 2014; Janowski, 2015; Gil-Garcia et al., 2018; Meijer, 2015). More recent work has focused on algorithmic government, techno-legal assemblages, platformization, and the governance of AI in the public sector (Yeung, 2018; Cobbe et al., 2021; Giest & Samuels, 2023; Kim & Ahn, 2025; Goossens et al., 2025). What remains insufficiently integrated, particularly for journals at the intersection of society, law, and policy, is a systematic account of how legal doctrine and policy design must co-evolve if digital transformation is to remain compatible with democratic public administration.

This article addresses that gap. It treats digital governance as an institutional transformation that reallocates discretion, redefines evidence, and reshapes accountability. The analysis is organized around two interlocking clusters of problems. The first cluster is legal: rule of law and legality in automated settings; data protection and surveillance; due process and explainability; liability and the outsourcing of public power; and cybersecurity as a condition of administrative continuity. The second cluster is policy-oriented: institutional capacity and legacy systems; digital inequality; interoperability and whole-of-government coordination; trust and participation; and cross-border regulatory fragmentation. The argument is that neither cluster can be solved in isolation. A technically elegant platform that cannot be explained in court is a legal failure. A legally meticulous statute that cannot be implemented by under-resourced agencies is a policy failure. Effective digital governance requires both enforceable legal constraints and capable, inclusive public institutions.

The contribution is threefold. First, the article clarifies the conceptual shift from e-government to digital governance and explains why that shift matters for administrative law. Second, it synthesizes legal and policy challenges into a coherent map that can be used by scholars, legislators, and public managers. Third, it advances recommendations that are deliberately institutional rather than merely rhetorical: statutory duties for algorithmic systems used in public functions; procurement rules that preserve auditability; layered human oversight calibrated to risk; digital public infrastructure designed as a public good; and evaluation regimes that treat fairness, contestability, and inclusion as performance criteria rather than afterthoughts. Throughout, the article remains comparative in orientation but does not assume that a single regulatory model can be transplanted without regard to constitutional tradition, administrative capacity, or social context.

1.1 Research Questions

RQ1. How does digital transformation alter the location and exercise of administrative discretion?

RQ2. What legal problems do automated and data-driven administrative systems create for legality, reasons, evidence, procedural fairness and judicial review?

RQ3. How should legal responsibility be allocated when public functions are technologically outsourced across agencies, vendors and infrastructure providers?

RQ4. What institutional safeguards can reconcile digital efficiency with equality, data protection, cybersecurity, accessibility and administrative justice?

RQ5. What lessons does Pakistan's Digital Nation Pakistan Act, 2025 provide for the legal governance of expanding digital public infrastructure?

1.2 Research Objectives

The article aims to (i) develop an administrative-law account of the relocation of discretion in digital government; (ii) identify doctrinal gaps concerning automated decisions, reasons and the administrative record; (iii) compare selected regulatory responses without ranking jurisdictions; (iv) develop institutional safeguards for procurement, oversight and digital inclusion; and (v) apply those findings to Pakistan.

1.3 Scope and Contribution

The article is deliberately concerned with public administration rather than digital regulation in general. Its original contribution is to treat algorithmic decision-making, data governance, procurement, digital infrastructure and administrative justice as parts of one accountability chain. The central proposition is that administrative law must follow public power through the socio-technical system in which it is actually exercised, rather than stopping at the identity of the official who signs the final decision.

2. From E-Government to Digital Governance: A Conceptual Framework

2.1 Defining the Field

Terminology in this field is unstable, and the instability is not merely semantic. E-government typically refers to the use of information and communication technologies to deliver government information and services, often with an emphasis on websites, portals, and transaction efficiency (Layne & Lee, 2001; UN DESA, 2024). Digital government, in the OECD usage, goes further: it denotes the use of digital technologies as an integrated part of governments' modernization strategies, creating public value through user-driven services, data reuse, and organizational transformation (OECD, 2014, 2020). Digital governance is broader still. It encompasses not only the internal transformation of the state but also the governance of digital systems themselves and the ways digital infrastructures mediate relations among citizens, firms, and public authorities (Fountain, 2001; Milakovich, 2012; Giest & Roberge, 2025).

This article uses digital governance to capture three related phenomena. The first is the digitization of administrative processes: case management systems, online applications, electronic identity, e-payments, and digital archives. The second is the datafication of public action: the conversion of social life and administrative encounters into machine-readable traces that can be stored, linked, analyzed, and reused (Couldry & Mejias, 2019; Kitchin, 2014). The third is the algorithmization of discretion: the embedding of classification, scoring, ranking, prediction, and generation into official workflows, whether through relatively simple rule engines or through machine-learning models (Citron, 2008; Yeung, 2018; Coglianese & Lehr, 2017). These three phenomena travel together. Once records are digital, they become data. Once they become data, they invite automation. Once they are automated, the site of official judgment moves.

2.2 Public Administration as an Institutional Order, Not a Service Channel

Public administration is more than service delivery. It is the organized exercise of public authority under law. Classic accounts emphasize hierarchy, written files, impersonal rules, and a professional civil service as conditions for legality and predictability (Weber, 1978). Subsequent traditions stressed incrementalism, street-level discretion, New Public Management, collaborative governance, and public-value creation (Lindblom, 1959; Lipsky, 1980; Hood, 1991; Moore, 1995; Osborne, 2006). Digital transformation intersects each of these traditions. It can reinforce Weberian ambitions of consistency by encoding rules into software. It can also intensify street-level dilemmas by giving frontline workers dashboards that constrain or invisibly steer their judgment. It can serve managerial performance metrics while hollowing out professional judgment. It can enable collaboration through shared platforms while concentrating power in those who control the platform's architecture.

A useful way to frame the transformation is to distinguish tools from infrastructures. A tool is an application that an agency may adopt or discard with limited systemic effect. An infrastructure is a durable arrangement—identity, payments, registries, cloud hosting, data-exchange layers—on which many other functions depend (Plantin et al., 2018; Cordella & Paletti, 2019). Digital governance becomes constitutionally significant when tools harden into infrastructures. At that point, design choices about authentication, default settings, data categories, model thresholds, and interface architecture begin to operate like secondary legislation. They structure who can apply, how quickly a claim is processed, which errors are visible, and which forms of life are legible to the state (Scott, 1998; Fourcade & Gordon, 2020).

2.3 Public Value, Administrative Justice, and the Risk of Decoupling

Digital reformers often justify investment in terms of public value: better services, lower costs, greater transparency, and improved outcomes. That language is important, but it can obscure conflicts among values. Speed may compromise careful individualized assessment. Personalization may compromise equality. Data sharing may compromise confidentiality. Predictive targeting may compromise the presumption that each case should be judged on its own merits. Bannister and Connolly (2014) warned

that digital-era governance rhetoric frequently under-specifies the values at stake. A similar concern now appears in work on transparency–accountability decoupling: disclosure of information about a system does not, by itself, produce institutional answerability (Ananny & Crawford, 2018; Veale & Brass, 2019).

Administrative justice supplies a complementary vocabulary. It asks whether people can understand what the state is doing to them, whether they can participate in decisions that affect them, whether reasons are given, and whether an independent forum can correct error (Mashaw, 1983; Adler, 2010). Digital systems can improve administrative justice by making status information available, reducing informal gatekeeping, and creating audit trails. They can also degrade it by producing inscrutable outcomes, shrinking opportunities for oral explanation, and shifting disputes from hearings to user-support tickets. The framework adopted here therefore evaluates digital governance against a dual standard: public-value creation and administrative justice. A transformation that increases throughput while diminishing contestability is incomplete, and in constitutional systems committed to the rule of law it may be unlawful.

2.4 Techno-Legal Assemblages

Recent research on policymaking in the digital era has emphasized techno-legal assemblages: the entangled arrangements of statutes, standards, organizations, vendors, datasets, and technical artifacts that shape how digital policy is formulated and implemented (Cordella & Gualdi, 2025; see also Jasanoff, 2004). This concept is analytically useful because it resists two common mistakes. The first mistake is technological determinism, the belief that tools dictate institutional outcomes. The second is legal formalism, the belief that a well-drafted statute will automatically govern a complex socio-technical system. In practice, an algorithm used in social-security fraud detection is simultaneously a software object, a procurement artifact, a data-protection processing activity, a labor-saving device, a political signal of toughness or modernization, and a potential source of administrative injustice. Legal and policy analysis must therefore follow the assemblage rather than isolate a single component.

This perspective also clarifies why comparative borrowing is difficult. Estonia's X-Road, India's Aadhaar-linked service architecture, Singapore's smart-nation stack, the European Union's digital-identity and data-governance package, and various national AI strategies rest on different constitutional settlements, different histories of state capacity, and different political economies of technology procurement (Margetts & Naumann, 2017; Bhatia, 2019; OECD, 2025). Lessons can travel; models should not be copied as if they were software patches. The remainder of the article therefore identifies recurring legal and policy challenges that appear across systems, while remaining attentive to variation in institutional starting points.

3. Methodology

This article employs a qualitative, doctrinal, and comparative policy-analysis design appropriate to a legal-policy problem that cannot be reduced to a single empirical dataset. The study proceeds in four integrated steps. First, it undertakes a structured review of peer-reviewed scholarship and major institutional reports on digital government, algorithmic public administration, and technology regulation published principally between 2001 and 2026, with emphasis on work that addresses public-law values rather than purely managerial performance. Second, it conducts doctrinal analysis of key legal instruments and leading judicial interpretations that now structure digital public action, including the European Union's General Data Protection Regulation, the Artificial Intelligence Act, selected administrative-procedure rules on automated acts, and the Court of Justice's interpretation of automated decision-making in SCHUFA Holding and Others (2023). Third, it uses focused comparison of policy frameworks and implementation patterns drawn from international assessments, notably the United Nations E-Government Survey 2024 and OECD work on digital government and governing with artificial intelligence, in order to identify recurring institutional constraints rather than to rank countries. Fourth, it synthesizes these materials into an analytical map of legal and policy challenges and derives recommendations that are evaluated against

criteria of legality, administrative feasibility, inclusion, and democratic accountability. No primary survey or experimental study was conducted; the validity of the argument therefore rests on the coherence of the conceptual framework, the representativeness of the legal sources selected, and the consistency of the challenges identified across jurisdictions and literatures. This design is suitable for a research-journal article whose purpose is to clarify an evolving field and to propose institutionally grounded reform rather than to estimate causal effects of a particular digital intervention.

4. The Transformation of Public Administration in the Digital Age

4.1 Reconfiguring Organizational Form

Digital transformation rearranges the machinery of government. Traditional departments were organized around functions, statutes, and paper files. Digital government encourages organization around life events, shared data layers, and reusable services: birth, work, illness, housing, retirement, bereavement. That shift can reduce the burden on citizens who would otherwise navigate fragmented bureaucracies. It also requires new coordinating centers—digital agencies, chief data officers, interoperability boards, and cybersecurity authorities—that sit uneasily beside line ministries (Mergel et al., 2019; OECD, 2020). The resulting structure is often hybrid. Legacy hierarchies remain legally responsible, while operational control migrates to platform teams, vendors, and cross-cutting units that do not appear in the statutory map of the state.

This hybridity has consequences for responsibility. Ministerial accountability assumes that a minister can be asked why a decision was taken and can obtain an answer from officials. Platformized administration complicates that chain. A delay may be produced by an identity-verification vendor; a denial may be produced by a rules engine configured years earlier; a discriminatory pattern may emerge from training data collected by another agency for another purpose. The organization still has a letterhead, but the decision process is distributed. Unless accountability mechanisms are redesigned to follow the actual path of decision-making, digital government can produce what might be called responsibility without control and control without responsibility.

4.2 Changing the Nature of Discretion

Street-level bureaucracy scholarship showed that frontline workers exercise discretion because rules are incomplete, cases are particular, and resources are scarce (Lipsky, 1980). Digital systems do not abolish discretion; they relocate and reshape it. Coders, data scientists, product managers, procurement officers, and vendors exercise design discretion when they choose features, thresholds, default values, and exception pathways (Citron, 2008; Bovens & Zouridis, 2002; Zouridis et al., 2020). Frontline workers may retain residual discretion, but it is often exercised in the shadow of a system recommendation, a risk score, or a lock that prevents an officer from proceeding without additional justification. The officer's discretion becomes a duty to accept or override a machine output rather than a duty to assemble the case from the beginning.

This relocation matters because design discretion is typically less visible than street-level discretion. A caseworker's harshness can be observed in an interview. A threshold buried in a model or a business-rule table may never be published, may be protected as a trade secret, and may change through software updates without a formal amendment to the governing scheme. Administrative law has long accepted that not every internal instruction must be gazetted. It has not yet fully adapted to a world in which internal instructions are executable code with population-scale effects. The transformation of discretion is therefore not only a management issue; it is a legality issue.

4.3 Evidence, Knowledge, and the Administrative Record

Public administration depends on an official record: the set of facts, findings, and reasons that can justify a decision and enable review. Digital systems alter what counts as a record. Click logs, model features,

confidence scores, and data-lineage metadata may be more informative than the short narrative an officer types into a decision letter. Conversely, the visible letter may conceal the system's actual grounds. If judicial review and internal audit continue to look only at the human-readable output, they will inspect a performance of reasoning rather than the reasoning itself (Oswald, 2018; Cobbe et al., 2021).

There is a further epistemic shift. Predictive tools invite agencies to act on probabilities about future behavior rather than on findings about past or present legal facts. A fraud-risk model does not determine that a claimant has committed fraud; it estimates that the claimant resembles previous cases labeled as risky. Using such estimates to prioritize investigation can be legitimate. Using them as substitutes for proof threatens the distinction between suspicion and finding, which is central to fair administration. The more public agencies rely on prediction, the more they need legal rules that specify what a score may and may not do.

4.4 The Citizen as User, Data Subject, and Rights Holder

Digital government often recasts the citizen as a user. User-centered design can be a genuine improvement on bureaucratic indifference. It can also shrink citizenship to consumer experience. A user has usability problems; a citizen has rights. A user wants a smoother journey; a citizen may need to refuse a journey that is unfair, inaccessible, or unlawfully intrusive. The same person is also a data subject with interests in purpose limitation, minimization, and objection, and a rights holder with interests in equality, dignity, and an effective remedy (Bennett & Raab, 2020; van Dijk, 2020). Policy documents that speak only the language of user satisfaction tend to undercount these other statuses.

This recasting has particular implications for vulnerable groups. People with unstable housing, limited literacy, irregular connectivity, disabilities, or reasons to distrust the state are less likely to complete digital journeys designed around an implied ideal user: documented, connected, linguistically fluent, and administratively confident. If those groups then face slower analog alternatives or are pushed into digital channels by default, the transformation redistributes administrative burdens downward (Herd & Moynihan, 2018). Digital governance that is serious about public administration cannot treat inclusion as a communications afterthought. It must treat it as a design constraint with legal force.

5. Legal Challenges

5.1 Legality, the Rule of Law, and Encoded Discretion

The principle of legality requires that public authorities act within the powers conferred by law and that those powers be sufficiently determinate to guide officials and constrain arbitrariness. Digital systems pressure this principle in two directions. First, they can increase formal consistency by applying the same encoded rule to large volumes of cases, reducing some forms of personal bias and informal favoritism. Second, they can conceal the real operative rule. When software implements a statute, the statute is no longer the only source of the norm. The code becomes a practical source of law for the people subject to it (Lessig, 2006; Hildebrandt, 2015). If the code diverges from the statute—through oversimplification, outdated updates, or silent policy choices—the administration may be acting through an unauthorized secondary code.

A related difficulty is authorization. Many digital tools are introduced under general statutory powers to administer a scheme, manage records, or improve efficiency. Those general powers were drafted for human offices, filing systems, and modest information technologies. They did not contemplate population-scale profiling, biometric identity, continuous monitoring of service use, or generative systems that draft official reasons. A legality-preserving approach would require clearer statutory predicates for high-impact digital practices, including the purposes for which data may be linked, the kinds of automation permitted, and the safeguards that must accompany them. In the absence of such predicates, agencies are tempted to

treat digital innovation as inherent in existing mandates. Courts may eventually disagree, but judicial correction arrives after systems have already become infrastructural.

The rule of law also requires prospectivity and intelligibility. People should be able to know the legal consequences of their actions and the criteria by which the state will assess them. Machine-learning systems that update continuously, or that rely on features with no intuitive relationship to the statutory criteria, strain this requirement. Even rule-based systems can become unintelligible when thousands of interacting business rules accumulate without systematic restatement in public language. Intelligibility is not a demand that every citizen read source code. It is a demand that the legally relevant criteria, the main data sources, and the consequences of automation be stated in a form that affected persons, advisers, and reviewing courts can use.

5.2 Automated Decision-Making, Due Process, and the Right to a Human Encounter

Due process and its administrative analogues—the right to be heard, the right to reasons, and the right to an impartial decision-maker—were designed around human proceedings. Automated systems unsettle each element. Hearing rights presuppose that there is a moment at which a person can put a case before the official mind that will decide. If the operative decision is produced before that encounter, or if the official mind is confined to a narrow override, the hearing may become ceremonial. Reason-giving presupposes that the decision-maker can state the grounds in a way that makes review possible. A generic statement that "the system assessed the application as ineligible" is not a reason in the administrative-law sense. Impartiality presupposes a decision-maker capable of considering the particular case rather than merely reproducing a statistical association.

Article 22 of the General Data Protection Regulation established an influential, if incomplete, template: as a rule, a data subject should not be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects the person, subject to specified exceptions and safeguards (Regulation 2016/679, art. 22). The Court of Justice's judgment in SCHUFA Holding and Others (2023) confirmed that the concept of automated individual decision-making can reach the generation of a probability value where that value plays a determining role in a subsequent decision. The ruling is significant for public administration even though the immediate facts concerned commercial credit scoring. It rejects a formalistic view that human involvement at the last moment automatically removes a process from the automated-decision category. Token human review does not restore due process.

Public-law systems outside the European Union face the same functional problem under different doctrinal labels. If an agency uses a model to rank inspection targets, deny licenses, flag welfare claims, or assess immigration risk, the question is whether affected persons can understand the case against them and contest the decisive inferences. Meaningful human involvement requires more than a signature. It requires time, competence, authority to depart from the system, access to the material facts, and a record of why an override was or was not exercised (Wagner, 2019; Green & Chen, 2019). Where caseloads are high and dashboards are designed to discourage deviation, human-in-the-loop arrangements can become human-on-the-loop decorations.

Explainability sits at the junction of due process and technology. There is an important distinction between model interpretability in a technical sense and legal reason-giving. An agency may not need to disclose every weight in a model. It does need to disclose the legally salient factors, the source and quality of the data, the known limitations, and the way the output was used in the particular case. Trade-secret claims by vendors cannot be allowed to extinguish the public duty to justify official action. If a tool cannot be explained to the degree required for lawful administration and fair review, it is not fit for use in that administrative function, regardless of its predictive performance.

5.3 Data Protection, Purpose Limitation, and the Surveillance Temptation

Digital public administration is data-hungry. Interoperability, once-only principles, personalization, and analytics all encourage the linkage of records that were previously separated by organizational boundaries. Data protection law seeks to discipline that hunger through principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability (Regulation 2016/679, art. 5; OECD, 2013). These principles are not anti-digital. They are an attempt to keep informational power compatible with personal autonomy and limited government.

The central legal tension is purpose limitation. A dataset assembled to pay a benefit can become useful for fraud detection, urban planning, tax compliance, public-health surveillance, or political intelligence. Each additional use may be attractive in isolation. Cumulatively, they can produce a de facto population register with secondary enforcement functions that were never authorized when the original data were collected. Function creep is therefore not an accidental by-product of digital government; it is a predictable institutional incentive. Legal systems that rely solely on broad "public interest" justifications will not constrain that incentive. They need purpose-specific authorizations, compatibility tests with real bite, and independent oversight capable of seeing across agencies rather than only within them.

Accuracy obligations acquire new urgency when data quality determines legal outcomes. Administrative data are often incomplete, outdated, or coded for operational convenience rather than for later inference. If an address field was never intended to measure household composition, its reuse in a risk model may systematically disadvantage mobile or multi-family households. Data-protection law's accuracy principle and administrative law's duty of careful inquiry converge here. An agency that automates on top of dirty data is not merely inefficient; it may be making unlawful findings.

Surveillance is the sharp edge of the same problem. Digital service channels, sensors, and analytics can convert ordinary administration into continuous observation. Location data from a public-mobility app, biometric check-ins at offices, metadata from benefit accounts, and social-media intelligence gathered for "integrity" purposes can accumulate into a portrait of private life. Democratic public administration requires a distinction between knowing enough to administer a law and knowing as much as technically possible. Without that distinction, the service state slides toward the supervisory state, and trust in digital channels declines precisely among those who most need public services.

5.4 Equality, Discrimination, and Algorithmic Bias

Equality before the law is a core administrative value. Digital systems can advance it by reducing the space for idiosyncratic prejudice. They can also industrialize discrimination by embedding historical inequalities in data and then applying those patterns at scale (Barocas & Selbst, 2016; Eubanks, 2018; Noble, 2018). Bias may enter through under-representation of certain groups in training data, through proxies that stand in for protected characteristics, through labeling practices that reflect prior enforcement priorities, or through user interfaces that are harder for some populations to complete. The resulting harm is often statistical rather than avowedly hostile, which makes it easier to deny and harder to litigate.

Anti-discrimination law is only partly adapted to this setting. Many doctrines look for a comparator, an identifiable decision-maker, and a relatively discrete act. Algorithmic harm may be distributed across a pipeline, produced by variables that are facially neutral, and visible only in aggregate disparities. Public-sector equality duties, disparate-impact analysis, and data-protection rules on sensitive-data processing offer partial tools, but they require agencies to measure outcomes they may not wish to see. A legally adequate digital administration would treat bias testing as a continuing official duty, not a one-time vendor assurance at procurement. It would also recognize that fairness metrics themselves encode value choices: equalizing false-positive rates, false-negative rates, or calibration across groups can yield different distributions of error (Kleinberg et al., 2017). Those choices belong in public policy, not only in technical appendices.

There is a further equality issue that is not about model bias as such: channel inequality. If the fastest, most complete, and most advantageous pathway is digital, then those who remain on analog or assisted pathways receive a thinner form of citizenship. Language minorities, older persons, persons with disabilities, rural residents, and low-income households are routinely at risk. Accessibility law and universal-design standards are therefore not peripheral compliance items. They are equality law for digital public administration. An inaccessible benefits portal can be as exclusionary as an inaccessible government building.

5.5 Accountability, Liability, and the Outsourcing of Public Power

A defining feature of public administration is that power is accompanied by answerability. Digital transformation complicates answerability because the actors multiply. An agency may own the statutory function, a systems integrator may own the platform, a cloud provider may own the environment, a model vendor may own the algorithm, and an open-source community may own components of the stack. When an unlawful decision or a security failure occurs, affected persons need a public counterpart who cannot hide behind the complexity of the chain.

Public law already contains doctrines that prevent the state from escaping its duties by contracting out. Those doctrines must be applied with renewed force. Procurement of an algorithmic tool used to determine legal entitlements is not equivalent to procurement of office furniture. It is a delegation of public power and should be treated as such. Contracts should preserve the agency's right to audit, explain, test, and, if necessary, discontinue the system. They should prohibit contractual confidentiality clauses from overriding disclosure duties owed to courts, auditors, ombuds institutions, and affected persons. They should allocate responsibility for data quality, model updates, security patches, and documentation in a way that matches operational control.

Liability law remains underdeveloped. Tort, state-liability, and data-protection-compensation regimes can address some harms, but they struggle with causation in composite systems and with damages that take the form of delayed benefits, dignitary injury, or chilled exercise of rights. Administrative remedies—reopening of decisions, interim payments, and systemic orders to correct a model—are often more important than damages. A mature legal framework would combine individual redress with powers to require model withdrawal, retraining, or structural change when a system produces recurring injustice. Accountability that ends with an apology and a software note is not accountability in the public-law sense.

Oversight institutions need complementary mandates. Data-protection authorities see processing risks; auditors see value for money and control failures; ombuds institutions see maladministration; courts see individual legality; sector regulators see domain-specific harm. Algorithmic public administration cuts across all of these. Without coordination, each body will inspect a fragment. With coordination, there is a risk of overlapping burdens that freeze innovation. The legal design problem is therefore to create interoperable oversight rather than either a vacuum or a pile of disconnected investigations.

5.6 Cybersecurity, Continuity of Government, and Digital Sovereignty

Once public administration depends on digital infrastructures, cybersecurity becomes a condition of legality and service continuity rather than a technical specialty. Ransomware, supply-chain attacks, insider misuse, and cascading cloud outages can halt benefit payments, hospital administration, tax collection, and identity verification. The legal questions that follow are immediate. What are the state's duties to maintain essential services during an incident? When must the public be notified? How should emergency analog procedures be pre-authorized so that officials are not forced to choose between paralysis and extra-legal improvisation? What minimum security standards should bind vendors who hold public data or operate critical administrative platforms?

Digital sovereignty debates add a geopolitical layer. Governments worry about dependence on a small number of foreign cloud and software providers, about extraterritorial data access by other states, and

about the loss of capacity to inspect or switch systems. These worries can be exaggerated into protectionism, but they are not imaginary. A state that cannot obtain logs, cannot port data, or cannot reconstruct a decision after a vendor withdraws has compromised its own administrative autonomy. Legal policy should therefore treat portability, escrow of critical documentation, audit rights, and exit planning as public-law requirements for essential systems, not as optional commercial terms.

5.7 Transparency, Official Secrets, and the Limits of Openness

Transparency is routinely listed among the benefits of digital government. Portals can publish budgets, performance data, and service standards. Open-data programs can enable reuse and external scrutiny. Yet the same digital environment creates new arguments for secrecy: model integrity, fraud prevention, cybersecurity, commercial confidentiality, and the protection of investigative methods. Some of these arguments are sound. Publishing every risk-indicator used in tax-audit selection would invite evasion. Others are opportunistic. Agencies and vendors may treat opacity as a convenience.

The legal task is to differentiate levels of disclosure. System-level transparency concerns the existence of a tool, its purpose, the legal basis, the categories of data, the human-review arrangements, and known limitations. Case-level transparency concerns the facts and inferences used in a particular determination. Technical transparency, shared with qualified auditors or courts under protected procedures, concerns code, features, and validation materials that cannot safely be dumped into the public domain. A binary choice between full openness and complete secrecy is a false choice. Administrative law already knows how to handle sensitive evidence in other domains; it can adapt those techniques rather than accept black-box government as a new normal.

6. Policy Challenges

6.1 Institutional Capacity, Skills, and Legacy Systems

Many legal failures of digital government begin as capacity failures. Agencies are asked to deploy advanced systems while still running fragmented legacy databases, paper-adjacent workflows, and workforces trained for a previous administrative era. OECD analysis of AI in government has emphasized that public-sector adoption trails the private sector in part because of skills shortages, outdated systems, constrained data, fiscal limits, and higher duties regarding privacy, transparency, and representation (OECD, 2024, 2025). These constraints are not excuses for lawlessness, but they are facts that policy must confront. A statute that demands explainable, unbiased, fully documented automation will remain ornamental if ministries cannot hire or retain people who can test a model, read a data-quality report, or challenge a vendor's claims.

Capacity is uneven within states as well as among them. Central digital agencies may accumulate talent while local governments, social-service offices, and small regulators remain dependent on consultants. The United Nations has stressed that local e-government development is essential and that gaps persist for least developed countries, African states, and small island developing states even as global averages improve (UN DESA, 2024). Policy that concentrates on flagship national apps therefore misses the administrative reality in which most people meet the state: municipal licensing, local social assistance, school administration, and primary healthcare. Transformation strategies need a territorial and multi-level dimension.

Legacy systems pose a distinctive policy trap. They are expensive to maintain, difficult to secure, and hostile to interoperability. Replacing them is also expensive, politically unglamorous, and operationally risky. Governments therefore add digital façades—new portals sitting on old databases—which create an impression of transformation while leaving the data architecture incoherent. The policy implication is that digital governance requires long-horizon investment in registers, identity, payments, and data standards,

not only in citizen-facing interfaces. Without that investment, law will demand accountability from systems that cannot produce a reliable audit trail.

6.2 The Digital Divide and Administrative Burden

Digital inequality is commonly discussed as a matter of access to devices and broadband. In public administration it is also a matter of administrative burden: the learning costs, compliance costs, and psychological costs of interacting with government (Herd & Moynihan, 2018). A portal that requires frequent authentication, scanned documents in specific formats, stable addresses, and uninterrupted sessions shifts burden onto the claimant. Those least able to bear the burden are often those with the strongest legal entitlements to support.

Policy responses that merely advertise digital literacy campaigns are insufficient. Literacy matters, but so do default channel design, assisted-digital services, offline equivalence, and the prohibition of digital-only access to essential entitlements unless an equally effective alternative exists. Inclusive design should be tested with actual excluded users rather than with internal staff playing the role of the public. Languages, disability access, low-bandwidth versions, and in-person support are part of the service, not optional extras. Where governments measure only digital take-up, they will celebrate a migration that may conceal abandonment by those who dropped out of the journey.

There is also a gender and social-reproduction dimension that policy documents often treat lightly. Women, caregivers, and informal workers may have less uninterrupted time, less control over devices, and greater exposure to identity-related risks within households. Migrant workers may fear that service data will migrate into enforcement systems. Persons with psychosocial disabilities may find chatbot-first design uniquely hostile. Digital governance policy that is not informed by these patterned experiences will reproduce them.

6.3 Interoperability, Data Governance, and Whole-of-Government Coordination

Few contemporary digital-government strategies omit interoperability. The once-only principle—that citizens should not have to supply the same information repeatedly—is attractive and, in the European Union, has been given legislative expression in the Single Digital Gateway framework and related data-exchange work. Yet interoperability is not a technical setting. It is a political settlement about which agencies may see which data, under whose authority, with what logs, and for what purposes. Without that settlement, calls for seamless government become calls for weakly governed data fusion.

Effective data governance for public administration requires several policy instruments at once: canonical base registers with clear custodians; quality standards and correction pathways; data-sharing agreements that specify purpose and retention; unique but privacy-preserving identifiers or tokenized exchange; and logging that makes secondary use reconstructable. It also requires a cultural change. Agencies that treat data as a proprietary asset will sabotage whole-of-government services. Agencies that treat all data as a common pool will violate purpose limitation. The policy art is to build shared infrastructure with differentiated access.

Coordination failures are visible in the proliferation of overlapping portals, inconsistent identity requirements, and duplicated analytics programs. They are also visible in the opposite problem: highly centralized platforms that become single points of failure and single points of political control. Neither extreme is attractive. Federated architectures with common standards can preserve departmental responsibility while enabling reuse. They demand, however, a center that can set standards and a periphery that has the capacity to implement them. Many governments have one without the other.

6.4 Trust, Legitimacy, and Citizen Participation

Trust is both an input and an output of digital governance. People will not use systems they regard as extractive or error-prone; systems that are underused then fail to deliver the efficiencies that justified

them. OECD survey evidence has shown limited public confidence that governments will use personal data only for legitimate purposes and limited trust that governments will regulate new technologies well, even where publics believe adaptation to automation should be a national priority (OECD, 2024, 2026). This is a legitimacy problem, not a marketing problem.

Legitimacy in public administration has always depended on more than outcomes. Procedure, fairness, and the sense that officials are acting in a public rather than a factional interest matter independently (Tyler, 2006). Digital systems can support these sources of legitimacy by making status visible, reducing petty corruption at the counter, and enabling faster correction of some errors. They can undermine them when people experience decisions as emanating from an unreachable machine, when errors are difficult to correct, or when digital identity becomes a condition of civic life. The policy implication is that trust-building must be designed into operations: rapid human escalation, published error rates, independent complaint pathways, and visible correction of systemic faults.

Participation is the neglected twin of user research. Consultations on digital strategy often gather the already connected. Co-design with affected communities, including those who have been harmed by earlier systems, is rarer and more valuable. Participatory mechanisms are not a substitute for legal rights, but they can surface failure modes that internal teams will not see. They can also discipline the rhetoric of inevitability. If a community can show that a predictive tool will intensify policing of poverty, the policy question is not only whether the tool is accurate but whether the intervention is just.

6.5 Procurement, Markets, and Public-Interest Technology

The market structure of digital government is concentrated. A small number of firms dominate cloud hosting, enterprise software, and advanced analytics. Public buyers are often weaker than their suppliers in technical expertise and contract negotiation. The result can be lock-in, escalating license costs, and systems that cannot be independently examined. Policy instruments exist—open standards, modular procurement, public-interest technology offices, in-house product teams, and strategic use of open-source components—but they require political backing against the convenience of turnkey deals.

Procurement is also a policy lever for rights protection. Bid specifications can require documentation, evaluation datasets, accessibility, logging, human-override design, and exit plans. Evaluation committees can include legal, social-policy, and user-advocate expertise rather than only information-technology staff. Payment schedules can be tied to performance against fairness and reliability criteria, not only against delivery milestones. Used this way, procurement becomes a form of regulation by contract. Used carelessly, it becomes the channel through which public power is privatized without a privatization debate.

6.6 Policy Fragmentation and Transnational Regulation

Digital systems do not respect jurisdictional borders, but public law does. Data may be stored in one country, processed in another, and used to determine rights in a third. Models trained on one population may be sold for use in another. Regulatory approaches now range from comprehensive legislative regimes, as in the European Union's combination of data protection, data governance, digital services, digital markets, and AI rules, to sectoral guidance, voluntary codes, and strategy documents elsewhere (Regulation 2022/2065; Regulation 2022/1925; Regulation 2024/1689; OECD, 2025). This diversity is inevitable in a world of different constitutional systems. It nevertheless creates compliance complexity for public administrations that use global tools and creates opportunities for regulatory arbitrage by vendors.

International organizations have attempted to supply common principles: the OECD Recommendation on Digital Government Strategies, the OECD AI Principles as updated in 2024, UNESCO's Recommendation on the Ethics of Artificial Intelligence, and United Nations processes on safe, secure, and trustworthy AI (OECD, 2014, 2024; UNESCO, 2021; United Nations, 2024). Principles help, but public administration needs operational rules. A ministry facing a procurement deadline cannot administer a principle. The policy

challenge is to translate transnational norms into domestic administrative practice without assuming that every jurisdiction can or should reproduce the European legislative acquis.

Fragmentation also exists inside single systems. Cybersecurity rules, records laws, privacy statutes, equality duties, procurement codes, and administrative-procedure acts were rarely designed as a package. Digital projects therefore encounter a thicket of overlapping approvals that can delay beneficial systems while still failing to stop harmful ones. Regulatory mapping—identifying which duties apply to which class of system—is becoming a necessary policy capability (OECD, 2025). Without it, officials either freeze or improvise.

7. A Comparative Regulatory Landscape

7.1 The European Union as a Dense Legal Order

The European Union has assembled the most elaborate binding framework for digital public and private power. The General Data Protection Regulation remains the backbone for personal-data processing, including rules on automated decision-making, data-protection impact assessment, and independent supervision. The Data Governance Act and Data Act address reuse and sharing of data. The Digital Services Act and Digital Markets Act regulate platforms and gatekeepers. The Artificial Intelligence Act introduces a risk-based scheme that treats certain public-sector AI uses as high-risk and imposes duties regarding data quality, documentation, transparency, human oversight, and post-market monitoring (Regulation 2024/1689). For public administration, the significance of this package is not only the content of individual instruments but their cumulative attempt to make digital systems legally describable.

Density brings costs. Agencies must interpret overlapping definitions of high-risk systems, profiling, public-interest processing, and essential services. They must also reconcile Union law with national administrative-procedure traditions, including those that have already authorized fully automated administrative acts in limited domains. The European trajectory nevertheless offers a lesson for other systems: if digital tools are going to exercise public power, they need legal categories that distinguish chatbot conveniences from systems that determine access to benefits, status, or sanctions. A single ethics charter will not carry that distinction.

7.2 Administrative-Law Adaptations and Judicial Signals

National administrative law has begun to adapt in uneven ways. Some systems have inserted explicit provisions on automated administrative acts, typically requiring that automation remain within tightly bound statutory criteria and that affected persons retain access to review. Courts have signaled that fundamental rights and legality do not recede because a process is automated. The functional message of recent European case law on scoring is that legal characterization follows practical effect. If a computational output determines a person's position, the law will treat it as a decision even if a human later transmits the result.

This effect-based approach is healthier than a metaphysics of human versus machine. It asks what the system does in the world. Public administrations that design processes to evade automated-decision rules by inserting a ritual click are learning the wrong lesson. The better lesson is to decide, up front, which functions may be automated, which require structured human judgment, and which should remain analog or hybrid because the stakes or the context cannot be captured by available data.

7.3 Strategies, Soft Law, and the Implementation Gap

Outside dense legislative orders, digital governance often proceeds through national AI strategies, digital-government roadmaps, ethical principles, and pilot projects. These instruments can mobilize investment and coordinate ministries. They are weaker at creating rights and remedies. The recurring pattern is an implementation gap: ambitious strategy documents, under-specified legal bases, limited evaluation, and

pilot systems that become permanent without a second look. The UN Survey's emphasis on a digital-government model framework and on AI's double-edged implications is useful precisely because it insists on planning, assessment, and risk management rather than on adoption for its own sake (UN DESA, 2024).

Developing and middle-income administrations face the gap in a sharper form. They are encouraged to leapfrog to advanced digital identity and platform government while legal aid, independent regulators, records management, and local administrative capacity remain thin. In that setting, a sophisticated identity system can improve inclusion and simultaneously expand exclusion if authentication failures block access to food, work, or health services (Bhatia, 2019; Drèze et al., 2017). Comparative policy analysis should therefore treat legal safeguards and grievance systems as part of the core stack, equal in importance to connectivity and applications.

7.4 What Comparison Does and Does Not Teach

Comparison teaches that certain problems are structural: encoded discretion, function creep, vendor opacity, digital exclusion, and oversight fragmentation appear across income levels and constitutional families. Comparison also teaches that solutions are path-dependent. A jurisdiction with a strong information commissioner, active administrative courts, and a tradition of reasoned decisions can extend those institutions to algorithmic systems. A jurisdiction that already struggles to enforce ordinary administrative legality will not be rescued by an AI ethics board. The practical implication is sequencing. Before governments automate high-stakes determinations, they should be able to explain ordinary determinations, correct ordinary data errors, and provide ordinary hearings. Digital transformation magnifies the quality of the underlying administrative state; it does not replace that state.

8. Pakistan: Digital Nation, Digital Public Infrastructure and Administrative Accountability

Pakistan is an important application of the article's framework because digital-government infrastructure is expanding through a statutory architecture that did not previously exist in this form. The National Assembly records the Digital Nation Pakistan Act, 2025 as Act No. I of 2025, enacted on 29 January 2025 (National Assembly of Pakistan, 2025).

The Act establishes the National Digital Commission and Pakistan Digital Authority and provides an institutional framework for digital society, digital economy and digital governance. It also contemplates a Data Exchange Layer for standardized sharing and integration of data among government entities and public-sector organizations. These mechanisms may improve service coordination, but they also create questions concerning legal authority, purpose limitation, access controls, auditability, data quality, retention and individual remedies.

Pakistan's constitutional framework supplies relevant legal principles. Article 4 requires that individuals be dealt with in accordance with law; Article 9 protects life and liberty; Article 10A protects fair trial and due process; Article 14 protects dignity and the privacy of home; Article 19A concerns access to information; and Article 25 guarantees equality before law and equal protection of law (Constitution of the Islamic Republic of Pakistan, 1973). These provisions should not be described as creating a complete statutory data-protection code. Rather, they provide constitutional standards against which digital administrative practices and future legislation may be evaluated.

The legislative position on personal data protection also requires precision. The Senate's official bill record states that the Personal Data Protection Bill, 2023 was introduced on 13 February 2023, was neither passed nor rejected by the committee, and consequently stood withdrawn from the committee (Senate of Pakistan, 2023). It should therefore be described as a legislative proposal rather than enacted law.

This creates a sequencing problem for Pakistan. Digital identity, data exchange and interoperable public services can become infrastructural before the legal rules governing their secondary use and correction are fully developed. High-impact data linkage and automated decisions should therefore have a clearly identifiable statutory basis; public bodies should maintain auditable records of material automated processing; individuals should have accessible routes to correction and human reconsideration; and public procurement contracts should preserve audit, disclosure, portability and exit rights.

The Pakistan case also strengthens the article's broader contribution. The relevant question is not whether Pakistan should copy the European Union. It is whether its developing digital public infrastructure can be made compatible with legality, equality, privacy, reason-giving and effective review within Pakistan's own constitutional and administrative framework.

9. Comparative Findings

The comparison supports four findings. First, digital transformation relocates discretion rather than eliminating it. Second, automated decision-making exposes a gap between technical transparency and legally sufficient reasons. Third, outsourcing can distribute operational control without transferring ultimate public-law responsibility. Fourth, digital inclusion and data governance are not peripheral policy issues: they affect whether legal entitlements can be exercised in practice.

Table 1. *Comparative overview of the legal governance of digital public administration*

Issue	EU	US/California	India	Estonia / platform model	Pakistan
Legal basis for automation	GDPR + AI Act where applicable + national administrative law	Constitutional, sectoral and state rules	Statutory + delegated framework	Infrastructure-led model with strong digital-state architecture	Emerging statutory digital-governance framework
Automated decisions	Art. 22 GDPR and AI Act controls where applicable	Fragmented/sectoral	Developing statutory safeguards	Depends on legal context	Needs clearer public-sector safeguards
Data governance	GDPR + data-governance instruments	Sectoral and state privacy regimes	Statutory data-fiduciary framework	Interoperability architecture	Digital Nation Act + incomplete comprehensive privacy framework
Oversight	Independent supervisory authorities + courts	FTC/state agencies/courts	Data Protection Board framework	Digital-government institutions + general law	PDA/NDC plus existing administrative institutions
Principal issue	Complexity and multi-level regulation	Fragmentation and coverage	State exemptions and implementation	Central coordination and infrastructure dependence	Sequencing infrastructure with rights and remedies

10. Recommendations

The following recommendations are addressed to legislators, central digital authorities, line ministries, oversight bodies, and, where relevant, courts. They are designed as a package. Isolated ethics guidelines will not compensate for weak statutory bases; isolated statutes will not compensate for missing skills and inaccessible services.

10.1 Enact Specific Legal Bases for High-Impact Administrative Automation

General mandates to administer a statute should not be treated as sufficient authority for high-impact automated decision-making, large-scale data linkage, or biometric identification in ordinary service contexts. Legislatures should specify which administrative functions may be automated, which data sources may be used, what human-review rights attach, and how long outputs and logs must be retained. Sunset and re-authorization requirements are appropriate for novel systems whose effects cannot be

known in advance. The aim is not to freeze innovation. The aim is to restore the connection between public power and democratic warrant.

10.2 Treat Algorithmic Systems Used in Public Functions as Reviewable Administrative Infrastructure

Agencies should maintain a public inventory of algorithmic systems that materially influence official action, including purpose, legal basis, data categories, human-oversight arrangements, and a contact point for challenge. For high-impact systems, they should produce and periodically update impact assessments covering legality, data protection, equality, accuracy, security, and accessibility. Those assessments should be available to auditors and, in appropriately redacted form, to the public. Courts and tribunals should be empowered to require production of the administrative record in its digital sense: the data, rules, model documentation, and override history relevant to the case, under procedures that protect genuinely sensitive material without annihilating review.

10.3 Redefine Meaningful Human Involvement

Where human oversight is required, it should be substantive rather than merely formal. Whether a particular human intervention is legally sufficient depends on the applicable legal regime, but a reviewer who lacks information, competence or authority to depart from the system cannot provide meaningful independent reconsideration.

10.4 Modernize Administrative Procedure for Digital Records and Reasons

Administrative-procedure codes should be amended to recognize electronic records, automated drafts, and system logs as part of the official file. Reason-giving duties should specify that a person is entitled to the legally salient factors, the principal data sources, and an explanation of how automation was used in the case. Agencies should be required to maintain version control of rules engines and models so that a decision can later be reconstructed. Without reconstructability there is no genuine appeal.

10.5 Align Procurement with Public-Law Duties

Model clauses for public-sector algorithmic procurement should guarantee audit rights, documentation, portability, accessibility, security standards, and the primacy of disclosure duties over vendor confidentiality. Evaluation should include legal and social-impact expertise. Essential systems should have exit and escrow plans. Where a vendor cannot provide the explainability required for lawful administration, the tool should be ineligible for that use case. Governments should also invest in internal product and data capacity so that they are intelligent customers rather than captive ones.

10.6 Build Inclusive Digital Public Infrastructure

Identity, payments, registries, and data-exchange layers should be designed as public infrastructure with universal-service characteristics. Essential entitlements must remain obtainable through assisted-digital and offline channels of equivalent effectiveness. Accessibility, language, low-bandwidth design, and disability support should be mandatory acceptance criteria, not later remediation. Performance management should track not only digital take-up but completion rates, error rates, appeal outcomes, and disparities across demographic and territorial groups. A system that performs well on average while failing systematically for identified groups is not a successful transformation.

10.7 Constrain Function Creep through Purpose Architecture

Data-sharing frameworks should be purpose-built rather than open-ended. Secondary uses that convert service data into enforcement intelligence should require explicit legal authority, necessity and proportionality analysis, and independent authorization where the risk to rights is high. Correction rights must be practically exercisable, including where data have already propagated across agencies. Logging of

access and reuse should be the default. The once-only principle should be implemented as a convenience for residents, not as a warrant for indiscriminate internal circulation of their lives.

10.8 Create Coordinated but Distinct Oversight

Rather than inventing a single all-purpose algorithm regulator in every jurisdiction, governments should assign clear lead roles and require structured cooperation among data-protection authorities, auditors, ombuds institutions, equality bodies, and sector regulators. Joint inspections, shared technical talent, and referral protocols can reduce both gaps and duplication. Parliaments should receive periodic reports on high-impact administrative systems, including known harms and remedial actions. Oversight that never reaches the legislature will not discipline the executive.

10.9 Invest in Administrative Capacity before Scaling High-Risk Tools

Skills, data quality, records management, and local implementation capacity are preconditions. National strategies should fund these foundations rather than only flagship applications. Regulatory sandboxes may be useful for testing, but they should not become permanent exemptions. Evaluation should be independent enough to recommend discontinuation. The politically difficult recommendation is the most important: some tools should not be scaled. A model that cannot meet legality, fairness, and contestability standards in a pilot will not acquire those virtues through wider deployment.

10.10 Embed Public Value and Administrative Justice in Evaluation

Digital-government success metrics should expand beyond cost, speed, and user-satisfaction scores. They should include accuracy of determinations, time to correct error, accessibility of remedies, distributional impacts, security incidents, and public understanding of rights. These metrics should inform budget decisions. What is not measured in digital government is soon treated as unimportant. If administrative justice is not measured, it will be traded away for throughput.

11. Conclusion

Digital transformation changes the institutional location of administrative power. The analysis has shown that the movement from paper files and individual officers toward interoperable databases, rule engines, predictive models and vendor-operated platforms does not remove discretion; it redistributes it. Choices about datasets, thresholds, defaults, model design, procurement and interface architecture can materially influence legal outcomes even when a statute continues to assign formal responsibility to a ministry or officer.

The first research question is answered by the concept of relocated discretion. The relevant administrative actors now include not only frontline officials but also policy designers, data managers, software teams, procurement officers and private contractors. The second is answered through the analysis of legality, reasons and the administrative record: digital decisions must remain connected to identifiable legal authority, intelligible criteria and records capable of meaningful review. The third is answered by the outsourcing analysis: contractual delegation may distribute operational control, but it should not extinguish the public authority's legal responsibility for decisions taken in its name.

The fourth research question requires an integrated response. Data protection, equality, cybersecurity, procurement, accessibility and administrative procedure should be treated as interconnected safeguards. Meaningful human review is important where the applicable legal framework requires it, but it should be defined by actual capacity to reconsider rather than by a formal signature. Transparency should likewise be layered: system-level information can be public, case-level reasons should be available to affected persons, and technical materials can be disclosed to courts or auditors through protected procedures where necessary.

The fifth question is illustrated by Pakistan. The Digital Nation Pakistan Act, 2025 creates a significant statutory architecture for digital governance, including the National Digital Commission, Pakistan Digital Authority and interoperable data infrastructure. At the same time, the Senate's official record confirms that the Personal Data Protection Bill, 2023 did not become enacted comprehensive legislation. Pakistan therefore illustrates the importance of sequencing: digital public infrastructure can generate durable administrative dependencies, making it preferable to develop legal safeguards, auditability and remedies alongside infrastructure rather than after deployment.

The article's principal contribution is consequently a legal-institutional framework for following public power through the complete digital decision chain. The framework does not require every jurisdiction to reproduce the European model. It requires that high-impact digital administration remain authorised by law, reconstructable for review, subject to meaningful accountability, accessible to affected persons and supported by institutions capable of correction. Digital government should be evaluated not only by speed and uptake but also by legality, contestability, equality, security and the ability of a person to obtain an effective remedy.

References

Adler, M. (2010). Understanding and analysing administrative justice. In M. Adler (Ed.), *Administrative justice in context* (pp. 129–159). Hart Publishing.

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society, 20*(3), 973–989. https://doi.org/10.1177/1461444816676645

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

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732. https://doi.org/10.15779/Z38BG31

Bennett, C. J., & Raab, C. D. (2020). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance, 14*(3), 447–464. https://doi.org/10.1111/rego.12222

Bhatia, G. (2019). *The transformative constitution: A radical biography in nine acts*. HarperCollins India.

Bovens, M., & Zouridis, S. (2002). From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control. *Public Administration Review, 62*(2), 174–184. https://doi.org/10.1111/0033-3352.00168

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

Cobbe, J., Lee, M. S. A., & Singh, J. (2021). Reviewable automated decision-making: A framework for accountable algorithmic systems. *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 598–609. https://doi.org/10.1145/3442188.3445921

Coglianese, C., & Lehr, D. (2017). Regulating by robot: Administrative decision making in the machine-learning era. *Georgetown Law Journal, 105*(5), 1147–1223.

Cordella, A., & Gualdi, F. (2025). Policymaking in the digital era: Exploring techno-legal assemblages and their impact on policy formulation. *Government Information Quarterly, 42*(2), 102023. https://doi.org/10.1016/j.giq.2025.102023

Cordella, A., & Paletti, A. (2019). Government as a platform, orchestration, and public value creation: The Italian case. *Government Information Quarterly, 36*(4), 101409. https://doi.org/10.1016/j.giq.2019.101409

Couldry, N., & Mejias, V. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Drèze, J., Khalid, N., Khera, R., & Somanchi, A. (2017). Aadhaar and food security in Jharkhand: Pain without gain? *Economic & Political Weekly, 52*(50), 50–60.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—Long live digital-era governance. *Journal of Public Administration Research and Theory, 16*(3), 467–494. https://doi.org/10.1093/jopart/mui057

Eifert, M., Metzger, A., Schweitzer, H., & Wagner, G. (2021). Taming the giants: The DMA/DSA package. *Common Market Law Review, 58*(4), 987–1028.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Fountain, J. E. (2001). *Building the virtual state: Information technology and institutional change*. Brookings Institution Press.

Fourcade, M., & Gordon, J. (2020). Learning like a state: Statecraft in the digital age. *Journal of Law and Political Economy, 1*(1), 78–108. https://doi.org/10.5070/LP61150258

Giest, S., & Roberge, I. (Eds.). (2025). *The Routledge international handbook of public administration and digital governance*. Routledge. https://doi.org/10.4324/9781003458081

Giest, S., & Samuels, A. (2023). Administrative burden in digital public service delivery: The social infrastructure of library programs for e-inclusion. *Review of Policy Research, 40*(5), 626–645. https://doi.org/10.1111/ropr.12516

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: Finding the crossroads. *Public Management Review, 20*(5), 633–646. https://doi.org/10.1080/14719037.2017.1327181

Goossens, J., Keymolen, E., & Stanojević, A. (Eds.). (2025). *Public governance and emerging technologies: Values, trust, and regulatory compliance*. Springer. https://doi.org/10.1007/978-3-031-84748-6

Green, B., & Chen, Y. (2019). Disparate interactions: An algorithm-in-the-loop analysis of fairness in risk assessments. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 90–99. https://doi.org/10.1145/3287560.3287563

Herd, P., & Moynihan, D. P. (2018). *Administrative burden: Policymaking by other means*. Russell Sage Foundation.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Edward Elgar.

Hood, C. (1991). A public management for all seasons? *Public Administration, 69*(1), 3–19. https://doi.org/10.1111/j.1467-9299.1991.tb00779.x

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly, 32*(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

Jasanoff, S. (Ed.). (2004). *States of knowledge: The co-production of science and social order*. Routledge.

Kim, Y., & Ahn, M. J. (2025). Digital governance and technological revolution: An introduction. In Y. Kim & M. J. Ahn (Eds.), *The art of digital governance: Navigating platforms and AI revolution* (pp. 1–13). Springer. https://doi.org/10.1007/978-3-032-00514-4_1

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. SAGE.

Kleinberg, J., Mullainathan, S., & Raghavan, M. (2017). Inherent trade-offs in the fair determination of risk scores. *Proceedings of Innovations in Theoretical Computer Science*. https://doi.org/10.4230/LIPIcs.ITCS.2017.43

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18*(2), 122–136. https://doi.org/10.1016/S0740-624X(01)00066-1

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Lindblom, C. E. (1959). The science of "muddling through." *Public Administration Review, 19*(2), 79–88. https://doi.org/10.2307/973677

Lipsky, M. (1980). *Street-level bureaucracy: Dilemmas of the individual in public services*. Russell Sage Foundation.

Margetts, H., & Naumann, A. (2017). *Government as a platform: What can Estonia show the world?* Oxford Internet Institute, University of Oxford.

Mashaw, J. L. (1983). *Bureaucratic justice: Managing social security disability claims*. Yale University Press.

Meijer, A. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly, 32*(2), 198–206. https://doi.org/10.1016/j.giq.2015.01.001

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

Milakovich, M. E. (2012). *Digital governance: New technologies for improving public service and participation*. Routledge.

Moore, M. H. (1995). *Creating public value: Strategic management in government*. Harvard University Press.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

Organisation for Economic Co-operation and Development. (2013). *The OECD privacy framework*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2014). *Recommendation of the Council on digital government strategies (OECD/LEGAL/0406)*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*. OECD Publishing. https://doi.org/10.1787/f64fed2a-en

Organisation for Economic Co-operation and Development. (2024). *Governing with artificial intelligence: Are governments ready?* OECD Publishing.

Organisation for Economic Co-operation and Development. (2025). *Governing with artificial intelligence: The state of play and way forward in core government functions*. OECD Publishing. https://doi.org/10.1787/795de142-en

Organisation for Economic Co-operation and Development. (2026). *Digital government outlook 2026: From foundations to transformational impact*. OECD Publishing. https://doi.org/10.1787/0496b2bc-en

Osborne, S. P. (2006). The new public governance? *Public Management Review, 8*(3), 377–387. https://doi.org/10.1080/14719030600853022

Oswald, M. (2018). Algorithm-assisted decision-making in the public sector: Framing the issues using administrative law rules governing discretionary power. *Philosophical Transactions of the Royal Society A, 376*(2128), 20170359. https://doi.org/10.1098/rsta.2017.0359

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

Pakistan. (2025). *Digital Nation Pakistan Act, 2025* (Act No. I of 2025).

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society, 20*(1), 293–310. https://doi.org/10.1177/1461444816661553

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), 2022 O.J. (L 265) 1.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689).

SCHUFA Holding and Others (Scoring), Case C-634/21, ECLI:EU:C:2023:957 (Court of Justice of the European Union, December 7, 2023).

Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press.

Senate of Pakistan. (2023). *The Personal Data Protection Bill, 2023: Bill summary and legislative status*.

Tyler, T. R. (2006). *Why people obey the law*. Princeton University Press.

United Nations. (2024). Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (G.A. Res. 78/265).

United Nations Department of Economic and Social Affairs. (2024). *United Nations E-government survey 2024: Accelerating digital transformation for sustainable development*. United Nations. https://doi.org/10.18356/9789213589793

United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.

van Dijk, J. (2020). *The digital divide*. Polity.

Veale, M., & Brass, I. (2019). Administration by algorithm? Public management meets public sector machine learning. In K. Yeung & M. Lodge (Eds.), *Algorithmic regulation* (pp. 121–149). Oxford University Press.

Wagner, B. (2019). Liable, but not in control? Ensuring meaningful human agency in automated decision-making systems. *Policy & Internet, 11*(1), 104–122. https://doi.org/10.1002/poi3.198

Weber, M. (1978). *Economy and society: An outline of interpretive sociology* (G. Roth & C. Wittich, Eds.). University of California Press. (Original work published 1922)

Wischmeyer, T. (2020). Artificial intelligence and transparency: Opening the black box. In T. Wischmeyer & T. Rademacher (Eds.), *Regulating artificial intelligence* (pp. 75–101). Springer.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance, 12*(4), 505–523. https://doi.org/10.1111/rego.12158

Zouridis, S., van Eck, M., & Bovens, M. (2020). Automated discretion. In T. Evans & P. Hupe (Eds.), *Discretion and the quest for controlled freedom* (pp. 313–329). Palgrave Macmillan.

// DECLARATIONS

▸ **Funding**	This research received no specific grant from any funding agency.
▸ **Conflict of Interest**	The authors declare that they have no known financial or personal conflicts of interest that could have influenced the work reported in this paper.
▸ **Data Availability Statement**	No new data were created or analysed in this study. The article is based on published legislation, judicial decisions, international standards and secondary literature cited in the references.
▸ **Ethical Statement**	Ethical approval was not required because the study is a doctrinal and comparative analysis of publicly available legal instruments, judicial decisions and published literature and did not involve human participants.
▸ **AI Use Disclosure**	Generative artificial intelligence tools were used in a limited and assistive capacity during the preparation of this manuscript, primarily for idea development, language refinement, and grammatical correction. The authors retain full responsibility for the originality, accuracy, analysis, interpretation, and final content of the manuscript.

// JOURNAL POLICIES *JuriSocial Journal of Criminology & Criminal Justice*

01 OPEN ACCESS & LICENCE
All articles are freely available on publication under CC BY-NC 4.0. Readers may share and adapt the work for non-commercial purposes with proper attribution.

02 COPYRIGHT
Authors retain copyright and grant JJCCJ the right of first publication.

03 PEER REVIEW
Every research article undergoes double-blind peer review by at least two independent reviewers.

04 PUBLICATION ETHICS
JJCCJ follows the Committee on Publication Ethics (COPE) Core Practices and guidelines.

05 PLAGIARISM POLICY
All submissions are screened with similarity-detection software; plagiarism in any form leads to rejection.

06 GENERATIVE AI POLICY
AI tools cannot be listed as authors. Any substantive use must be disclosed; authors remain fully responsible for the content.

07 CORRECTIONS & RETRACTIONS
Errors are corrected through published corrigenda; retractions follow COPE guidelines.

08 ARCHIVING & INDEXING
Content is preserved through [PKP Preservation Network / LOCKSS]. DOIs are registered with Crossref.

09 PUBLICATION CHARGES
No article publishing fee charged.

10 DISCLAIMER
The views expressed are those of the authors and do not necessarily reflect the views of the editors or the publisher.

SUBMISSIONS & ENQUIRIES ◆ https://Jurisocial.org